

Cryptocurrency as a Commodity: The CFTC’s Regulatory Framework

David Lucking & Vinod Aravind
Allen & Overy LLP

Introduction

Since Bitcoin emerged onto the scene approximately 10 years ago, multiple attempts have been made by U.S. regulators to categorise Bitcoin, as well as other cryptocurrencies, virtual currencies and digital tokens. Are instruments that take the form of peer-to-peer, open-source ledger technology securities, commodities, or assets that cannot be defined using existing regulatory definitions?

In this chapter, we examine how the U.S. Commodity Futures Trading Commission (CFTC), a regulator historically involved in the oversight of physical commodity markets – although since the advent of more esoteric commodity-linked products, such as listed derivatives (also known as futures) and over-the-counter swaps, also responsible for the oversight of those markets – determined that intangible cryptocurrency was a commodity. We view this move as prompted by a desire to police old-world commodity scams in nascent cryptocurrency markets. Over time, the CFTC’s enforcement actions have targeted activity ranging from the failure to register entities selling cryptocurrency-related products to scams involving a Bitcoin thief impersonating a federal employee. If the CFTC is to increase regulation of this evolving space, it will need both increased data on the cryptocurrency spot market (a point of the emphasis that is directly in conflict with virtual currencies’ structural emphasis on individual privacy) and greater delegation of power from legislators in order to keep up with technological shifts and new products, like Facebook’s proposed Libra currency.

The advent of CFTC regulation of cryptocurrencies

Cryptocurrency history

Bitcoin, the first implementation of a peer-to-peer, distributed ledger currency, was introduced in 2009. Unlike traditional fiat currencies, Bitcoin and similar cryptocurrencies such as Ether do not require a centralised authority to issue the new currency or confirm payment activities; instead, the network as a whole is involved in authorising transactions and generating new currency. Furthermore, the individuals trading the cryptocurrency on the blockchain may be anonymous (or at least “pseudonymous”, in that real-life identities are not disclosed).

From inception, the relative security and privacy offered by virtual currencies fuelled the illicit use of cryptocurrency as a mechanism to facilitate money laundering, trafficking, and sanction violations. In addition to the illicit use of cryptocurrencies, there was increasing scope to make money through market manipulation of these virtual currencies; for example, through classic “pump and dump” and fraudulent mis-selling schemes.

As they became aware of the need to regulate to protect investors and stifle money laundering and other criminal activity, U.S. regulators moved in a stop-start fashion to regulate

cryptocurrency. In 2015, the CFTC came forward and defined Bitcoin and other virtual currencies as commodities under the U.S. Commodity Exchange Act.¹

Defining cryptocurrency as a commodity

The CFTC was established in 1974 to provide oversight of markets previously under the jurisdiction of the U.S. Department of Agriculture. The CFTC has stated that to foster public interest and financially sound markets, it will act to “prevent price manipulation or any other disruptions to market integrity” and to “protect all market participants from fraudulent or other abusive sales practices”.² As a matter of jurisdiction, the CFTC is empowered to regulate “commodities” under the U.S. Commodity Exchange Act (the **CEA**), and has exclusive jurisdiction over “accounts, agreements [...] and transactions involving swaps or contracts of sale of a commodity for future delivery”. 7 U.S.C. § 2. The CFTC has also asserted jurisdiction over fraud and manipulation involving spot market transactions relating to commodities which underlie futures or swaps.

The CFTC first determined that Bitcoin and other virtual currencies are properly defined as “commodities” under the CEA in 2015 in an enforcement action, *In the Matter of: Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan, CFTC Docket No. 15-29*.³ In its settlement order, the CFTC stated that individuals who had created a platform for the purchase and sale of Bitcoin options were in fact operating a facility for the trading or processing of swaps without being registered as a swap execution facility or designated contract market. In doing so, the CFTC applied the broad definition of commodity as laid out in the CEA and found that the scope of that definition included Bitcoin: “The definition of a “commodity” is broad [...] Bitcoin and other virtual currencies are encompassed in the definition and properly defined as commodities.”

CFTC enforcement actions

Alan Greenspan once noted that: “corruption, embezzlement, fraud, these are all characteristics which exist everywhere. It is regrettably the way human nature functions, whether we like it or not. What successful economies do is keep it to a minimum. No one has ever eliminated any of that stuff.”⁴ Having found Bitcoin and similar virtual currencies to be “commodities”, the CFTC’s initial enforcement actions focused on classic fraud cases.

Early enforcement actions

The CFTC defined the scope of its cryptocurrency regulatory span with some early legal victories: *CFTC v. Dillon Michael Dean and The Entrepreneurs Headquarters Limited*,⁵ *CFTC v. Patrick K. McDonnell and CabbageTech*,⁶ *Corp. d/b/a Coin Drop Markets*, and *CFTC v. My Big Coin Pay, Inc.*⁷

In *Dean*, the CFTC’s complaint targeted an alleged Ponzi scheme for options fraud, failure to register as a Commodity Pool Operator (**CPO**) and as an Associated Person of a CPO, and CPO fraud. Dean and associates solicited investor funds (in the form of Bitcoin) by promising to deliver “a set return rate of 11%–17.5%/week depending on how much you invest” and to pay commissions for new investor referrals. The funds were not invested in the promised “binary option” investments, and no trading profits were made. When investors sought withdrawals, Dean alternately ignored requests; claimed the investor website had been hacked and infected by ransomware; and that the blockchain was just “SLOWWW”. While addressing a classic, common Ponzi scheme, the CFTC’s enforcement action also put trusts, syndicates, and similar actors in trading virtual currency derivatives or other commodity interests via pooled investor funds on notice that they need to register with the CFTC as a CPO.

The *McDonnell* litigation also related to Ponzi scheme activity. *McDonnell* was litigated as a bench trial in federal court in the Eastern District of New York, and featured similar facts to *Dean* (though *McDonnell* did not have the same creative excuses for failure to return investor funds). The *McDonnell* Court reaffirmed the *Derivabit* holding, applying deference to the Commission's interpretation of its jurisdictional statute ("The court generally defers to an agency's interpretation of a statute that the agency is responsible for administering") and re-affirming the CFTC's position that virtual currencies are commodities (citing, among other support, an *amicus* brief from the Chicago Mercantile Exchange). The Court also reaffirmed that the CFTC may take enforcement action over virtual currency fraud even where no derivatives are present, on the basis that 17 CFR 180.1 grants the CFTC antifraud authority over any "contract of sale of any commodity in interstate commerce" – not just futures contracts or swaps.

Finally, the determination in the *My Big Coin Pay, Inc.* case was a further step in reaffirming earlier decisions and action. The *Big Coin Pay* court found the CEA's text supports the CFTC's position, as the CEA defines "commodity" generally and categorically, "not by type, grade, quality, brand, producer, manufacturer, or form". Thus, the court reasoned that the CFTC's "broad approach" to its antifraud jurisdiction over virtual currencies is in sync with Congress's goal of "strengthening the federal regulation of the ... commodity futures trading industry".

Recent enforcement actions

Recent fraud actions have addressed even more brazen activity and highlight the need for continued enforcement action.

Perhaps the boldest fraud case to date involved Morgan Hunt and Kim Hecroft,⁸ who misrepresented their ability to invest and trade in commodity interests. Furthermore, the CFTC's complaint alleged that both defendants supplied their victims with phoney documents in furtherance of their fraud, including altered versions of a publicly available CFTC memorandum. This alteration was intended to mislead the defendants' victims into believing that they were required to pay a "tax obligation" to the CFTC if they wished to withdraw funds from their Bitcoin accounts. This "tax obligation" was, of course, payable in Bitcoin (that the defendants kept). Morgan and Hunt even arranged for an agent to impersonate a fake CFTC employee to attest to the validity of the tax and sent forged documents purportedly authored by the CFTC's general counsel.

A further example of CFTC enforcement actions of outright fraud related to cryptocurrency is the injunction order against Patrick K. McDonnell and his company doing business as Coin Drop Markets (**CDM**). McDonnell's and CDM's scheme induced customers to send both money and virtual currencies, supposedly in exchange for real-time virtual currency trading advice and virtual currency purchasing and trading carried out on behalf of the customers. However, the allegedly expert advice was never provided, and funds that were delivered to McDonnell and CDM to purchase or trade on customer's behalf simply disappeared.⁹

The Ponzi schemes identified by the CFTC for recent enforcement actions have grown in scale. The trading firm Gelfman Blueprint, Inc. and its CEO Nicholas Gelfman were ordered to pay over \$2.5 million for their Bitcoin Ponzi scheme. This scheme targeted and defrauded at least 80 people for more than \$600,000. The customers' funds were supposed to be placed in a pooled commodity fund that allegedly employed a high-frequency, algorithmic trading strategy executed by the defendants' computer trading program called "Jigsaw". In reality, the strategy was fake, the purported performance reports were also falsified, and the payouts

of the supposed profits to customers were in actuality the misappropriated funds from other customers.¹⁰

Failure to register under the Commodity Exchange Act

In addition to outright fraud and other manipulative actions, the CFTC has also sought to prevent entities from operating without the proper registration. Enforcement actions related to failure to register as a regulated exchange (e.g., either a swap execution facility or a designated contract market) or as a registered intermediary (e.g., a futures commission merchant) are often brought in connection with other frauds (in line with the early *Coinflip* action). Two of these actions include the foreign trading platforms 1 Pool Ltd. and the Bitcoin exchange Bitfinex.

1 Pool Ltd. was found to have illegally offered customers retail commodity transactions that were margined in Bitcoin and in doing so failed to register as a futures commission merchant (FCM). Furthermore, it did not have the required anti-money laundering procedures in place.¹¹

Similarly, Bitfinex operated as a platform of illegal off-exchange retail commodity transactions in Bitcoin and other cryptocurrencies, and failed to register as an FCM as required by the CEA.¹²

Bitfinex's platform allowed for spot and forward trading in Bitcoin; however, the platform also allowed users to borrow funds from other platform users in order to trade Bitcoin on a leveraged basis. Under the CEA, the CFTC has jurisdiction over such leveraged retail commodity transactions, unless "actual delivery" occurs within 28 days of execution. See 7 U.S.C. § 2(c)(2)(D). The CFTC noted that each Bitfinex customer interest relating to leveraged transactions was held for the benefit of the customer in an omnibus settlement wallet and "accounted for in real time on Bitfinex's database. However, the omnibus settlement wallet was owned and controlled by Bitfinex and Bitfinex held all 'private keys' associated with its omnibus settlement wallet". As a result, the CFTC found that no "actual delivery" occurred and that Bitfinex had violated the retail commodity transaction rules by providing for the execution and confirmation of leveraged retail commodity transactions without having such transactions occur on or subject to the rules of a CFTC-regulated exchange.

The Bitfinex enforcement is also an example of a regulator stretching to deal with novel regulatory issues and the market subsequently being forced to adjust. In the aftermath of the Bitfinex enforcement action, the CFTC received requests from market participants for guidance around the meaning of "actual delivery" in the specific context of virtual currency transactions. In response, the Commission issued a "proposed interpretation" of the term "actual delivery" consistent with the position it had taken in Bitfinex, with "actual delivery" occurring when the customer takes "possession and control" of the virtual currency.¹³

Future of CFTC enforcement relating to cryptocurrencies

While CFTC antifraud enforcement actions are on the rise, we expect the limits of the CFTC's jurisdiction over spot cryptocurrency transactions to be tested in the coming years. As former CFTC commissioner Timothy Massad has noted, there is "a problem for oversight generally and for the quality of crypto derivatives: if the underlying cash market is susceptible to (or characterized by) fraud and manipulation, then what confidence can one have in the derivatives?"¹⁴

As it moves forward, the CFTC is increasingly liaising with other regulators, including the Securities and Exchange Commission (SEC), to bring enforcement actions. SEC

Commissioner Jay Clayton has agreed that “[f]raud and manipulation involving Bitcoin traded in interstate commerce are appropriately within the purview of the CFTC, as is the regulation of commodity futures tied directly to Bitcoin”.¹⁵ In certain circumstances, the SEC has brought cases around violations of the securities laws (e.g., sales of “tokens” or security-based swaps without registration), including where the CFTC has also brought virtual currency actions for breach of the commodities laws.¹⁶ It seems, at least for now, that both regulators will continue to enforce their rules separately, without a single U.S. regulator taking precedence in the virtual currency space.

Priorities for new derivative product listings

The CFTC’s existing rules allow exchanges to “self-certify” new products for listing.¹⁷ As a result, a number of cryptocurrency-related products have been launched with relatively limited public input. (By contrast, the SEC has moved relatively slowly with respect to cryptocurrency-linked securities and has not approved Bitcoin-linked ETFs for trading on regulated exchanges.)

In response, on May 21, 2018 the CFTC issued a staff advisory (CFTC Letter No. 18-14)¹⁸ providing guidance for registered entities (e.g., designated contract markets and swap execution facilities) interested in listing virtual currency derivative products. In the advisory, the CFTC acknowledged that virtual currencies are “unlike any commodity that the CFTC has dealt with in the past”. In particular, the advisory noted that “it is more difficult to provide context or a frame of reference for the prices of virtual currency that are quoted on the spot markets. While prices and transactions on those spot markets can be observed, the connection of these prices to any commercial market, intrinsic value, or supply and demand is less clear than for other commodities”.

As a result, the CFTC stated that it believes that virtual currency exchanges will need to establish an “information sharing arrangement with the underlying spot market(s)” for virtual currencies in order to establish whether any pricing anomalies or market manipulation may be occurring. The CFTC also recommended that exchanges set large trader reporting thresholds at five Bitcoin and noted in a footnote that “traders subject to large trader reporting are subject to possible reporting of spot market activity”.

The advisory clearly indicates that the CFTC is increasingly looking for ways to obtain information around spot market activity in cryptocurrencies. If it obtains such information, cases around ‘spoofing’ or market manipulation in the spot markets may be soon to follow.¹⁹

Facebook’s Libra cryptocurrency

At the same time that the CFTC is looking for linkages between fraudulent cryptocurrency activity in the spot and futures/swaps markets, new products are forcing a re-evaluation of the Commission’s jurisdictional reach.

Facebook has announced plans to launch its own cryptocurrency, targeting the first half of 2020 for its debut. The company intends to share control of the cryptocurrency with a consortium that includes venture capital firms, credit card companies, and other tech giants including Visa, Mastercard, Paypal and Uber.²⁰

The stated mission of Libra is “a simple global currency and financial infrastructure that empowers billions of people”. In its white paper, Libra is described as a secure, scalable, and reliable blockchain, backed by a reserve of assets designed to give intrinsic value,²¹ and governed by the independent Libra Association tasked with evolving its financial ecosystem.²²

In response to the June 18, 2019 Facebook White Paper on Libra, CFTC Chairman Christopher Giancarlo said the agency was in the “very early stages of conversations” with

Facebook. At these early stages, it is unclear if Libra would fall under the CFTC's jurisdiction given its linkage to existing, regulated fiat currency and securities. Chairman Giancarlo noted that "if the cryptocurrency could be backed by the U.S. dollar, then there might be less of a need for derivatives tied to it...That's very clever".²³ One key question posed by regulators, which remains unanswered, is whether and how Facebook will put in place and follow anti-fraud, anti-money laundering and know-your-customer measures, and whether a truly supranational virtual currency like Libra could be structured outside of the U.S.'s regulatory reach.

* * *

Endnotes

1. *In the Matter of: Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan, CFTC Docket No. 15-29*. 2015 WL 5535736 (Sept. 17, 2015).
2. CFTC Backgrounder on Self-Certified Contracts for Bitcoin Products, https://www.cftc.gov/sites/default/files/idc/groups/public/@newsroom/documents/file/bitcoin_fact_sheet120117.pdf.
3. CFTC Docket No. 15-19, 2015 WL 5535736 (Sept. 17, 2015).
4. Alan Greenspan, interview on Amy Goodman's Democracy Now Sept. 24, 2007.
5. <https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfentrepreneurscomplt011818.pdf>.
6. <https://www.cftc.gov/PressRoom/PressReleases/pr7702-18>; 332 F.Supp.3d 641 (EDNY August 28, 2018).
7. https://www.cftc.gov/sites/default/files/2018-10/enfmybigcoinpayincmemorandum092618_0.pdf.
8. <https://www.cftc.gov/sites/default/files/2018-09/enfmorganhuntcomplaint092818.pdf>.
9. <https://www.cftc.gov/PressRoom/PressReleases/pr7675-18>.
10. <https://www.cftc.gov/PressRoom/PressReleases/7831-18>.
11. <https://www.cftc.gov/PressRoom/PressReleases/7886-19>.
12. <https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfbfxnaorder060216.pdf>.
13. <https://www.cftc.gov/sites/default/files/idc/groups/public/@lrfederalregister/documents/file/2017-27421a.pdf>.
14. <https://www.brookings.edu/wp-content/uploads/2019/03/Timothy-Massad-Its-Time-to-Strengthen-the-Regulation-of-Crypto-Assets-2.pdf>.
15. <https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11>.
16. Ipool Ltd., discussed *supra* endnote 11 above is an example; the SEC complaint relating to Ipool Ltd. offering security-based swaps in violation of the securities laws is available here: <https://www.sec.gov/litigation/complaints/2018/comp-pr2018-218.pdf>.
17. See 17 CFR 40.2.
18. https://www.cftc.gov/sites/default/files/idc/groups/public/%40lrlettergeneral/documents/letter/2018-05/18-14_0.pdf.
19. See also the CFTC's proposed interpretation around "actual delivery", *supra* note 13, at p. 60338 for an indication of the type of behaviour in the spot market that has

garnered CFTC attention (“[T]he emergence of these nascent markets has also been negatively marked by a variety of retail customer harm that warrants the Commission’s attention, including, among other things, flash crashes and other market disruptions, delayed settlements, alleged spoofing, hacks, alleged internal theft, alleged manipulation, smart contract coding vulnerabilities, bucket shop arrangements and other conflicts of interest” (internal citations omitted)).

20. <https://libra.org/en-US/white-paper/#introducing-libra>.
21. <https://libra.org/en-US/white-paper/#the-libra-currency-and-reserve>.
22. <https://libra.org/en-US/white-paper/#introducing-libra>.
23. <https://www.coindesk.com/facebook-holds-talks-with-cftc-over-globalcoin-crypto-currency-report>.

**David Lucking****Tel: +1 212 756 1157 / Email: david.lucking@allenoverly.com**

David is Head of Allen & Overy's U.S. International Capital Markets group. He has expertise in derivatives and structured finance transactions, as well as the regulatory framework that underpins the derivatives market. David advises financial institutions on a wide range of derivatives products and asset classes (including credit, rates, FX, longevity) in both funded and unfunded form. He has drafted a number of market standard document templates for the International Swaps and Derivatives Association, Inc. (ISDA) and other derivatives industry bodies. David is the U.S. adviser to the Credit Derivatives Determinations Committee which determines Credit Events and other matters for the credit derivatives market as a whole. David has advised on various aspects of the transition of the over-the-counter derivatives market to regulated trading platforms and central clearing houses, as well as the registration of a number of swap dealers under the Dodd-Frank Act.

**Vinod Aravind****Tel: +1 212 610 6498 / Email: vinod.aravind@allenoverly.com**

Vinod has experience representing commercial banks, institutional lenders, and multi-lateral agencies in connection with a variety of structured finance, derivatives, and debt capital markets transactions. He has also worked on ISDA documentation projects, including protocols relating to credit derivatives. Vinod also has experience advising U.S. and non-U.S. banks and other market participants on varied aspects of the Volcker Rule and the Dodd-Frank Act, including trade execution, clearing, business conduct, reporting and other regulatory requirements.

Allen & Overy LLP

1221 Avenue of the Americas, New York, NY 10020, USA
Tel: +1 212 610 6300 / URL: www.allenoverly.com

Crypto-Asset Trading Platforms: A Regulatory Trip Around the World

Todd W. Beauchamp, Stephen P. Wink and Simon Hawkins
Latham & Watkins LLP

Crypto-asset trading is a fast-growing part of the financial sector.¹ Some countries have wholeheartedly embraced crypto-assets; others have been more reticent to permit widespread adoption. Generally, countries have either interpreted existing laws and regulations to apply to crypto-assets or adopted new laws or regulations to specifically address crypto-assets – or embarked upon some combination of the two. Due to their use of blockchain and other distributed ledger technology, crypto-assets are, in most cases, inherently cross-border and cross-jurisdictional, and nothing but legal regimes keep them within certain borders. Thus, most issuers of crypto-assets and trading platforms must address multiple legal and regulatory frameworks when attempting to enter the market. This chapter will explore the regulation of crypto-asset trading platforms in the European Union, the United States, Hong Kong, Singapore, the Philippines, Thailand, and Japan.

European Union

The EU has an overarching financial regulatory framework principally made up of EU regulations (which are directly applicable in EU Member States) and EU directives (which must be adopted into national law by each Member State). While this framework ensures a degree of harmonisation across EU Member States, it does not guarantee uniform regulation. The regulation of crypto-assets provides a good illustration of this issue. A threshold question when considering whether EU financial regulation applies to crypto-assets is whether the crypto-asset in question constitutes a “financial instrument” or “electronic money”. A crypto-asset trading platform that facilitates trading in crypto-assets that are financial instruments or electronic money will typically be subject to licensing and other regulatory requirements. The definitions of financial instrument and electronic money are set out in Directive 2014/65/EU (“MiFID II”) and Directive 2009/110/EC (“2EMD”), respectively. EU Member States have interpreted and implemented these directives differently; thus, it is possible that the same crypto-asset could be a financial instrument in one jurisdiction and not in another.² In addition, national laws, such as long-standing domestic securities laws, financial promotion and public offer laws, and newly introduced laws or regulations specifically addressing crypto-assets, may impose regulation on instruments that fall outside the scope of MiFID II or 2EMD.³ Often, those jurisdictions that have not introduced crypto-asset-specific laws or regulations have issued guidance on the applicability of existing financial regulatory regimes to crypto-assets.⁴ In addition to the variance in national laws, this Member State-specific guidance increases the risk of regulatory divergence throughout the EU. Given this fragmentation, it is necessary to classify a given crypto-asset in accordance with the national laws of each EU Member State in which it is to be marketed, distributed, traded, or otherwise used.

The European Securities and Markets Authority (“ESMA”), which is the European Supervisory Authority (“ESA”) with jurisdiction over financial markets and investor protection in the EU, and the European Banking Authority (“EBA”), the ESA with jurisdiction over banking activity in the EU, both recently noted the fragmented state of affairs in their respective advice to the European Commission and European Parliament on regulating crypto-assets (“ESMA Advice”⁵ and “EBA Report”,⁶ respectively).

ESMA conducted a survey of 29 European regulators regarding the regulatory classification of six examples of existing crypto-assets (“Survey”) and concluded that the Member State regulators, “in the course of transposing [MiFID II] into their national laws, have in turn defined the term financial instrument differently. While some employ a restrictive list of examples to define transferable securities, others use broader interpretations. This creates challenges to both the regulation and to the supervision of crypto-assets”.⁷ The ESMA Advice highlighted areas of the EU regulatory framework (e.g., the requirements relating to settlement under the European Central Securities Depositories Regulation, which are critical to trading financial instruments in the EU) that may be difficult to apply to crypto-assets that are classified as transferable securities (a type of MiFID II financial instrument). The ESMA Advice also cautioned that the introduction of Member State-specific regulatory regimes to address crypto-assets will create an unequal playing field for crypto-assets across the EU. Considering the inherently cross-border nature of most crypto-assets, the ESMA Advice encouraged an “EU-wide approach” to the regulation of crypto-assets not otherwise captured by MiFID II and 2EMD.

While definitive classification remains subject to EU Member States’ laws, some high-level principles for classification of crypto-assets can be extracted from the Survey:

- ESMA did not include “pure payment-type” crypto-assets (such as Bitcoin, Ether, and Litecoin) in the Survey on the basis that they “are unlikely to qualify as financial instruments”.
- For a majority of the regulators surveyed, the existence of attached profit rights (whether or not alongside ownership or governance rights) was sufficient for a crypto-asset to constitute a transferable security, provided the crypto-asset was freely tradable and not a payment instrument.
- None of the regulators surveyed characterised “pure utility-type” crypto-assets as financial instruments on the basis that the “rights that they convey seem to be too far away from the financial and monetary structure of ... a financial instrument”.⁸

Similarly, while the EBA Report recognised that crypto-assets must be classified on a case-by-case basis, it stated that crypto-assets are not considered “funds”⁹ or equivalent to fiat currency in any EU Member State for the purposes of EU financial regulation,¹⁰ and indicated that crypto-assets are most likely to satisfy the definition of electronic money in circumstances where the value of the crypto-asset is pegged to the value of fiat currency (e.g. stablecoins) and the crypto-asset is redeemable for fiat currency.

Indeed, what the ESMA Advice and the EBA Report suggest is that for purposes of regulation, the characterisation of crypto-assets proceeds predominantly on the basis of an “intrinsic” assessment of a given crypto-asset, focused on the rights or entitlements granted to holders, rather than on the basis of “extrinsic” factors, such as the intended or actual use of the crypto-asset or other contextual factors relating to the crypto-asset (such as whether a platform to which the crypto-asset relates is currently operational or whether the network underlying the crypto-asset is decentralised).

Beyond the recent extension of EU anti-money laundering and counter-terrorism finance (“AML”) legislation to capture certain crypto-asset service providers who did not otherwise fall under the AML regime,¹¹ there has not been much movement to harmonise the treatment of crypto-assets across the EU. The European Commission and the European Parliament have not yet responded to the recommendations in the ESMA Advice or the EBA Report. Thus, while it seems likely that the EU will undertake further efforts to harmonise the regulation of crypto-assets across the EU, the timeline remains unclear.

United States

In the US, crypto-asset markets and related activities are regulated under several federal and state regulatory regimes. At the federal level, the Securities and Exchange Commission (“SEC”) is concerned with whether a crypto-asset is a “security”, the Commodity Futures Trading Commission (“CFTC”) asks whether a crypto-asset is a “commodity”, and the Treasury Department’s Financial Crimes Enforcement Network (“FinCEN”) regulates certain activities involving “convertible virtual currency”. A crypto-asset can be one or more of these things simultaneously, and may also be subject to any number of state-level money transmitter, securities, and tax regimes.

Acting as a Security. If a crypto-asset fits within the definition of a security, it is regulated by the SEC and subject to existing laws and regulations.¹² In this case, the issuer of the crypto-asset needs to either register the offering and sales of the crypto-asset under Section 5 of the Securities Act of 1933 or find an applicable exemption.¹³

In addition, the Securities Exchange Act of 1934 regulates intermediaries that engage in securities transactions. Many crypto-asset exchanges are thus required to register as a securities exchange or, depending on their business model, a broker-dealer.

Any funds that invest in crypto-assets that are securities are subject to the same laws applicable to pooled vehicles that invest in securities generally, such as the Investment Company Act of 1940 and the Investment Advisers Act of 1940.

Notably, while the SEC regulates crypto-assets that are deemed securities, the SEC staff has indicated that the two most well-known crypto-assets – Bitcoin and Ether – are not considered securities. If, however, these non-security crypto-assets were bundled into investment vehicles (such as exchange-traded funds), they would become securities and be subject to SEC regulation.

Acting as a Commodity. Generally, the CFTC has considered crypto-assets not otherwise designated as securities to be commodities (including Bitcoin and Ether). The CFTC regulates commodities, futures, options on futures, and swaps (i.e., derivatives) on commodities (including crypto-assets), subjecting market participants and their trades to regulatory oversight and registration requirements. The CFTC also regulates certain retail commodity transactions that are leveraged, financed, or margined as if they were futures. While the CFTC has no direct regulatory oversight of markets or platforms that conduct spot transactions of crypto-assets, the CFTC does retain the authority to police against manipulation and fraud in the spot commodities markets. Thus, the CFTC regulates the crypto-asset spot markets by enforcement, and has done so aggressively in the past few years.¹⁴

The CFTC also regulates exchanges that trade futures or options on crypto-assets as designated contract markets. The CFTC has issued a primer with respect to the heightened scrutiny of futures contracts on crypto-assets, and CFTC commissioners have publicly stated that the agency will be paying strict attention to this market.¹⁵ In its report on its examination

priorities for 2019, the CFTC's Division of Market Oversight listed cryptocurrency surveillance practices at the top.¹⁶

Acting as a Currency. If the crypto-asset is intended to act as a medium of exchange, it may be treated similarly to fiat currency for the purposes of the Bank Secrecy Act of 1970 and its implementing regulations (collectively, the "BSA"), which serves as the principal AML regulatory regime in the US.¹⁷

The BSA applies to "financial institutions", which includes banks and other entities, such as money services businesses ("MSBs").¹⁸ MSBs include multiple categories of entities, the most relevant to crypto-asset exchanges being a "money transmitter".¹⁹ A money transmitter is "[a] person that provides money transmission services",²⁰ which is, in turn, defined as "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means".²¹ Generally, any person falling within the definition of money transmitter must register with FinCEN and comply with the attendant requirements under the BSA. However, if an entity is functionally regulated by the SEC or the CFTC, it does not need to register as an MSB even if it otherwise meets the criteria.

The BSA does not expressly reference or contemplate crypto-assets or crypto-asset-related activities. FinCEN, however, has published guidance and issued administrative rulings that provide insight on the application of the BSA to certain crypto-asset-related activities. FinCEN's core guidance on the topic was published in 2013 ("2013 Guidance"),²² which introduced the term "convertible virtual currency"²³ and defined the following three types of participants in generic convertible virtual currency arrangements:

- A "user" is "a person that obtains virtual currency to purchase goods or services".
- An "exchanger" is "a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency".
- An "administrator" is "a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency".²⁴

FinCEN concluded that a user of convertible virtual currency is not an MSB, but that an administrator or exchanger of convertible virtual currency²⁵ that "(1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason is a money transmitter under FinCEN's regulations".²⁶

In May 2019, FinCEN consolidated its guidance and administrative rulings on crypto-asset-related activities ("2019 Guidance") and provided additional clarity regarding the application of the BSA to a variety of crypto-asset-related business models. Notably, the 2019 Guidance states that a crypto-asset trading platform that matches offers to buy and sell convertible virtual currency for fiat currency, for which the platform maintains a separate fiat currency wallet and virtual currency wallet for customers to use in connection with trades on the platform, is an exchanger and therefore must register with FinCEN as an MSB and comply with the BSA.²⁷ Generally, based on FinCEN's guidance, if a crypto-asset exchange buys or sells crypto-assets as a customer business or provides customers with a hosted wallet (or other stored value device), then it is a money transmitter under the BSA and must register with FinCEN and comply with the applicable rules. On the other hand, if the platform simply provides information and the opportunity for customers to match and execute their own trades, it is likely not a money transmitter.

Finally, US states and territories regulate the provision of money transmission services to residents of their respective jurisdictions.²⁸ Although the requirements and related definitions vary slightly from state to state, money transmission services typically include (i) traditional money remittance, (ii) issuing or selling open-loop stored value or prepaid access, or (iii) issuing or selling payment instruments. Generally, if an entity is engaged in any one of those activities, it must be (a) licensed as a money transmitter under the relevant state law, (b) appointed and serve as the authorised agent of a money transmitter licensed in the relevant state, or (c) an entity or activity that is exempt under the relevant money transmitter statute.

The states have not taken a uniform approach with respect to regulating the transmission of crypto-assets. Some states have expressly amended their existing money transmission statutes to contemplate crypto-assets, some have issued guidance and/or interpretations that incorporate crypto-assets into their current money transmission statutes, and others have issued guidance finding that crypto-asset-related activities are not money transmission under their statutes. The State of New York is unique in that the financial services regulator issued a stand-alone regulation specific to crypto-asset-related activities.²⁹ As a general rule though, if a trading platform is accepting money or crypto-assets from one person or place and storing it and/or sending it to another person or place, in most instances, that activity is money transmission.³⁰

Hong Kong

In Hong Kong, the Securities and Futures Commission (“SFC”) recently announced that it is exploring whether virtual asset trading platforms (“VA Platforms”)³¹ should be regulated under its existing powers and has set out a conceptual regulatory framework for doing so (“Conceptual Framework”).³² The SFC has created a regulatory sandbox (“VA Platform Sandbox”) for interested virtual asset trading platform operators (“VA Platform Operators”). The SFC will discuss its regulatory standards under the Conceptual Framework with participants and consider whether and how to regulate VA Platforms in light of the feedback it receives. If the SFC concludes that VA Platforms are suitable for regulation, it may begin granting licences to qualified VA Platform Operators. The SFC cannot currently regulate VA Platforms because existing laws and regulations extend only to certain types of financial products, such as securities, futures and funds.

Under the Conceptual Framework, a VA Platform Operator that offers trading in one or more crypto-assets that are securities (e.g., security tokens) will fall within the regulatory jurisdiction of the SFC and may apply to the SFC to be licensed. In granting a licence, the SFC will likely impose certain conditions, including that the VA Platform Operator will:

- Provide services only to “professional investors”.³³
- Admit only those crypto-assets issued under initial coin offerings (“ICO”) that meet certain conditions.
- Execute a trade only if the client’s account has sufficient assets to cover the trade.
- Maintain any additional financial resources as may be prescribed by the SFC.
- Maintain an insurance policy that would provide full coverage for crypto-assets held in cold storage and substantial coverage for crypto-assets held online.³⁴
- Perform all reasonable due diligence on crypto-assets before listing them on the VA Trading Platform and disclose the listing criteria to clients.
- Publish comprehensive trading rules on its website.

If a crypto-asset exchange facilitates the trading of crypto-assets that are not securities or another type of regulated product, the exchange is not regulated.

Singapore

In Singapore, the regulatory regime applicable to any crypto-asset exchange depends on what type of crypto-asset is being traded. A crypto-asset exchange that offers any “digital payment token service” is regulated under the Payment Services Act (“PSA”), which will come into effect this year. Under the PSA, a crypto-asset exchange that deals (i.e., buys and sells) digital payment tokens or facilitates the exchange of digital payment tokens on a regular, centralised basis will require a licence from the Monetary Authority of Singapore (“MAS”).

A crypto-asset exchange that facilitates trading in security tokens must apply to the MAS to become an approved exchange or a recognised market operator (“RMO”), unless otherwise exempted. In May 2018, the MAS proposed expanding the existing RMO regime from a single tier to three tiers to accurately reflect the risks posed by different market operators (“MOs”).³⁵ Under the current regime, RMOs are only permitted to deal with “accredited investors” and cannot deal with retail investors.³⁶ Under the proposed multitiered RMO regime, the permissible activities and customer base would vary depending on the tier:

- Tier 1 would be the most heavily regulated. A Tier 1 RMO would have limited access to Singapore-based retail investors and would thus be subject to more stringent regulatory requirements than other RMOs. A Tier 1 RMO would be required to comply with all the requirements imposed on Tier 2 RMOs, along with additional requirements designed to protect retail investors (e.g., prospectus requirements, continuing obligations, and change of control transactions).
- Tier 2 would capture those MOs that qualify under the existing RMO regime. MOs that are authorised under the existing RMO regime would be re-classified as Tier 2 RMOs.
- Tier 3 would be for smaller MOs that target the non-retail market segment (e.g., banks). Tier 3 RMO applicants would need to fulfill a reduced set of capital requirements under Singapore’s Securities and Futures Act and a simplified set of technology risk management and outsourcing compliance requirements. The application process for Tier 3 RMO applicants would also be simplified; they would be able to self-certify their compliance with a checklist of requirements prepared by the MAS. However, they would continue to be subject to the fit and proper requirements that are imposed on existing RMOs.³⁷

The Philippines

In the Philippines, the Bangko Sentral ng Pilipinas (“BSP”) regulates virtual currency exchange services (entities that convert crypto-assets to fiat currency and/or *vice versa*) as a type of remittance and transfer company (“RTC”). In addition to registering with the BSP, RTCs must comply with the virtual currency exchange-specific guidance published by the BSP.³⁸

Meanwhile, the Philippines Securities and Exchange Commission (“PSEC”) is due to issue final rules on digital asset offerings in the near future. The PSEC is also set to release draft rules to regulate other crypto-asset-related activities, such as crypto-asset exchanges and crowdfunding.

Additionally, the Philippines has created the Cagayan Economic Zone Authority (“CEZA”). However, a crypto-asset exchange registered with the CEZA may not service users in the Philippines, and any tokens to be traded must be listed on licensed off-shore exchanges. Thus, the utility of the CEZA is unclear.

Thailand

Digital asset business operators are required to obtain a licence from the Minister of Finance upon the recommendation of the Thailand Securities and Exchange Commission (“Thai SEC”).³⁹ To obtain a crypto-asset exchange licence, the company must, among other things:

- Be established under Thai law.
- Possess sufficient financial resources, as determined by the Thai SEC.
- Maintain policies, systems, and measures (such as IT systems and internal control measures) that comply with the Thai SEC’s standards.
- Ensure that adequate KYC and AML programmes are in place.

Japan

In Japan, crypto-asset exchanges⁴⁰ are required to be registered with the Financial Services Agency (“FSA”) under the Payment Services Act (“Japan PSA”).⁴¹ In March 2018, Japan’s existing registered crypto-asset exchanges created a self-regulatory body, the Japanese Virtual Currency Exchange Association (“JVCEA”), to provide additional regulation and guidance applicable to licensed crypto-asset exchanges. The FSA certified the JVCEA, which can now impose disciplinary sanctions on registered crypto-asset exchanges that do not comply with its regulation and guidance.

Furthermore, if the crypto-asset exchange trades crypto-assets that are securities that entitle investors to a distribution of profits or assets, both the crypto-asset exchange and the crypto-assets may be subject to regulations promulgated under the Financial Instruments and Exchange Act of Japan.

Conclusion

In most of the countries surveyed here, while some types of crypto-asset exchanges are currently regulated, most jurisdictions are still determining how to regulate without stifling innovation. In the EU, despite the existence of a centralised regulatory system, Member States have not been uniform in their interpretation of directives, leaving a crypto-asset exchange that hopes to operate EU-wide with the unenviable task of attempting to understand and comply with more than 20 regulatory regimes. In the US, the biggest takeaway is that all crypto-assets and crypto-asset exchanges will be captured under *some* regulatory regime, but it could be difficult to determine which one best applies (at both the federal and state level). In Hong Kong, regulators have created a sandbox to better tailor regulation to crypto-asset exchanges. The outcome of that experiment remains to be seen. In Singapore, the MAS is working on a new and more tailored regulatory regime to address the disparate needs of various crypto-asset exchanges. In the Philippines, other than regulating virtual currency exchanges, the government has not really addressed crypto-asset trading. In Thailand and Japan, crypto-asset exchanges are required to be registered (or licensed) with their respective regulator and meet ongoing compliance requirements, and are subject to enforcement.

While the vision of a global economy where crypto-assets offer instantaneous execution and borderless trades may still be a bit far off, the emergence of crypto-assets and trading of

these instruments is forcing countries to re-examine their existing legal and regulatory frameworks and their application to crypto-assets and the platforms that trade them. The next few years will be critical in the development of regulatory regimes addressing crypto-assets and crypto-asset trading platforms. Striking the right balance between consumer protection and market integrity and resilience without stifling innovation is the challenge all regulators face.

Acknowledgments

Yvette D. Valdez

Tel: +1 212 906 1797 / Email: yvette.valdez@lw.com

Yvette Valdez is a partner in the New York office of Latham & Watkins and a member of the Derivatives Practice and Financial Institutions and FinTech Industry Groups. Ms. Valdez advises emerging companies, financial institutions, and investment managers on complex regulatory challenges in the development of bespoke financial crypto-asset and cryptocurrency technologies, including token sales, market infrastructure, trading, clearing, and settlement solutions on distributed ledger technology. She also advises clients on domestic and cross-border fintech initiatives in the derivatives markets. In addition, Ms. Valdez has significant experience representing dealers, intermediaries, and end-users in connection with derivatives (swaps and futures) legal and regulatory matters under the Dodd-Frank Act, the Commodity Exchange Act, as well as related CFTC, SEC, and prudential regulation.

Nozomi Oda

Tel: +81 3 6212 7830 / Email: nozomi.oda@lw.com

Nozomi Oda is a partner in Latham & Watkins Gaikokuho Joint Enterprise in Tokyo. Ms. Oda's practice encompasses cross-border public and private M&A transactions, joint ventures, strategic investments, and capital markets transactions. Ms. Oda is the Local Chair of the Corporate Department in Tokyo. Ms. Oda regularly advises on a wide variety of Japanese regulations, including securities regulations, financial regulations, fund regulations, merger review, and healthcare and life sciences regulations. From 2009 to 2011, Ms. Oda was seconded to the Financial Services Agency of Japan ("FSA") as a deputy director of the corporate disclosure department.

Sam Maxson

Tel: +44 20 7710 1823 / Email: sam.maxson@lw.com

Sam Maxson is an associate in the London office of Latham & Watkins. Mr. Maxson regularly advises a wide range of clients (including banks, insurers, investment firms, financial markets infrastructure providers, and technology companies) on all aspects of financial regulation. Mr. Maxson has a particular focus on fintech and insurtech, advising both established and emerging businesses on the application of global financial regulation to new and novel uses of technology in finance and insurance. His expertise also extends to the increasingly widespread interest in crypto-assets and "tokenisation" of financial markets.

Kenneth Y.F. Hui

Tel: +852 2912 2711 / Email: kenneth.hui@lw.com

Kenneth Hui is an associate in the Hong Kong office of Latham & Watkins. Mr. Hui is a member of the Financial Institutions Group and focuses on advising domestic and foreign financial institutions on regulatory issues. Mr. Hui advises on a range of Hong Kong financial regulatory matters including licensing, marketing of products and services, conduct

of business, money laundering, market misconduct, investigations, and regulatory aspects of M&A deals and other transactions. Mr. Hui has previously advised banks, brokers, private equity funds, asset managers, insurance companies, and other companies on matters relating to the Securities and Futures Commission (“SFC”), Hong Kong Monetary Authority (“HKMA”), Insurance Authority, and other regulators.

Gen Huong Tan

Tel: +65 6437 5349 / Email: genhuong.tan@lw.com

Gen Huong Tan is an associate in the Singapore office of Latham & Watkins and a member of the firm’s Technology Transactions Practice. He has experience advising clients on data privacy matters, mergers and acquisitions, technology and commercial transactions.

Charles Weinstein

Tel: +1 202 637 3343 / Email: charles.weinstein@lw.com

Charles Weinstein is an associate in Latham & Watkins’ Washington, D.C. office and a member of the Financial Institutions Industry Group, FinTech Industry Group, and Payments & Emerging Financial Services Practice. Mr. Weinstein focuses primarily on regulatory, transactional, and enforcement matters related to electronic and mobile payments, money services businesses (“MSBs”), and other emerging payment technologies, including those related to money transmission, virtual currencies, payment instruments, and stored value offerings. Mr. Weinstein also has experience advising clients on consumer credit issues.

Loyal T. Horsley

Tel: +1 202 637 2396 / Email: loyal.horsley@lw.com

Loyal Horsley is an associate in the Washington, D.C. office of Latham & Watkins and a member of the Payments & Emerging Financial Services Practice and Financial Institutions Industry Group. Ms. Horsley’s practice focuses on a broad range of regulatory, transactional, and enforcement matters related to electronic and mobile payments, money services businesses, and other emerging payment technologies, including those related to money transmission, virtual currencies, payment instruments, and stored value offerings.

* * *

Endnotes

1. For ease of reading, we use the term “crypto-asset” as a catch-all for the variety of financial instruments that a cryptocurrency, token, or coin can represent, including currency, securities, and commodities. Some jurisdictions’ regulatory regimes differentiate between the type of instrument that is being traded, while others simply address the trading of crypto-assets, generally. If a governmental agency has defined a different term to capture the same concept, we have used that term in the discussion of that agency’s regulation of crypto-asset-related activities.
2. The same is true for electronic money, although the definition has been implemented with a greater degree of uniformity across EU Member States than the definition of financial instrument.
3. Examples of the former notably exist in Germany and Italy, while examples of the latter exist in France, Gibraltar, and Malta.

4. See, e.g. Financial Conduct Authority, *CP 19/3: Guidance on Cryptoassets* (Jan. 2019).
5. ESMA, *Advice – Initial Coin Offerings and Crypto-Assets* (Jan. 9, 2019).
6. EBA, *Report with advice for the European Commission on crypto-assets* (Jan. 9, 2019).
7. ESMA Advice, p. 5.
8. ESMA Advice, p. 20.
9. Unless they otherwise fall within the definition of electronic money.
10. A position with which both the Bank of England and the European Central Bank (as well as other Member State central banks and monetary authorities) have publicly concurred on many occasions.
11. Which has itself been affected through an EU directive (Directive (EU) 2018/843 (“5MLD”)) which is subject to implementation under the national law of EU Member States (some of which are likely to “gold-plate” the requirements).
12. Whether the crypto-asset is a security is decided pursuant to regulation but also to the threshold test imposed by the Supreme Court in *Securities and Exchange Commission v. W. J. Howey Co.*, 328 U.S. 293 (1946) (often referred to as the *Howey* test). Under the Securities Act of 1933, an instrument is an investment contract (or a security) if it is a “contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party”.
13. For example, SEC Regulation D and Regulation A both offer issuers potential exemptions.
14. See, e.g. *CFTC v. Patrick McDonnell and CabbageTech Corp. d/b/a Coin Drop Markets*, 18-CV-361, E.D.N.Y. (Mar. 6, 2018).
15. CFTC, *A CFTC Primer on Virtual Currencies*, Oct. 17, 2017.
16. CFTC, Release No. 7869-19, *CFTC Divisions Announce Examination Priorities*, Feb. 12, 2019.
17. FinCEN is responsible for administering the BSA.
18. 31 C.F.R. § 1010.100(ff).
19. *Id.* § 1010.100(ff)(5).
20. *Id.* § 1010.100(ff)(5)(i)(A).
21. *Id.*
22. FIN-2013-G001, *Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (Mar. 18, 2013).
23. In the 2013 Guidance and subsequent rulings, FinCEN distinguishes “convertible virtual currency” from “virtual currency”, neither of which are specifically referenced in the BSA. FinCEN defines “virtual currency” as “a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency”. “Convertible virtual currency” is more narrow and includes “virtual currency [that] either has an equivalent value in real currency, or acts as a substitute for real currency”. The 2013 Guidance and subsequent rulings address convertible virtual currency.
24. *Id.*

25. *Id.*
26. *Id.* (emphasis in original).
27. See FIN-2014-R011, *Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform* (Oct. 27, 2014).
28. Only the State of Montana does not regulate money transmission.
29. The New York State Department of Financial Services adopted an entirely new regulatory regime specific to crypto-assets acting as currency: the Virtual Currency Business Activity licence (“Bitlicense”) regime.
30. Some states have stated that their laws do not apply if there is no fiat currency involved in the transaction; see e.g. Pennsylvania Department of Banking and Securities, *Money Transmitter Act Guidance for Virtual Currency Businesses* (Jan. 23, 2019) and Texas Department of Banking, Supervisory Memo 1037, *Regulatory Treatment of Virtual Currencies Under the Texas Money Services Act* (April 1, 2019). Others have revised their statutes or issued interpretations to capture the activity; see e.g. Washington State, which defines “money transmission” in part as “receiving money or its equivalent value (*equivalent value includes virtual currency*) to transmit, deliver, or instruct to be delivered to another location ... by any means”. Wash. Rev. Code § 19.230.010(18) (emphasis added).
31. The SFC’s terms for crypto-asset trading platforms.
32. Securities and Futures Commission, *Statement on regulatory framework for virtual asset portfolio managers, fund distributors and trading platform operators*, Nov. 1, 2018.
33. Professional investors as defined under Part 1 Schedule 1 of the Securities and Futures Ordinance (Cap. 571) (“SFO”).
34. Cold storage refers to the offline storage of a crypto-asset, such as on a USB drive or in some physical form. See Latham & Watkins’ Book of Jargon: Cryptocurrency & Blockchain Technology for additional definitions.
35. While public comments are no longer being accepted, MAS has not yet published its response, and no bill has been introduced in Parliament to implement this proposal.
36. Accredited investors (both individuals and corporations) are defined in section 4A of the Securities and Futures Act and section 2 of the Securities and Futures (Classes of Investors) Regulations 2018.
37. The “fit and proper requirements” are the criteria that MAS expects all persons carrying out regulated activities to meet. These include, but are not limited to: the (i) honesty, integrity, and reputation; (ii) competence and capability; and (iii) financial soundness of the applicant. See MAS Guidelines on Fit and Proper Criteria.
38. BSP, Circular No. 942, Amendment to Section 4511N of the Manual of Regulations for Non-Bank Financial Institutions, Jan. 5, 2017; BSP, Circular No. 944, Guidelines for Virtual Currency (VC) Exchanges, Jan. 19, 2017.
39. Digital asset business operators include digital asset exchanges, brokers, dealers, and a catch-all for “other businesses relating to digital assets as prescribed by the Minister under the recommendation of the [Thai SEC]”. Emergency Decree on Digital Asset Businesses B.E. 2561 (2018).
40. A crypto-asset exchange is a service provider that engages in the sale, exchange, or brokerage of crypto-assets.

41. The Japan PSA only captures certain types of crypto-assets (those that satisfy all of the conditions in one of the two categories below) and only exchanges trading those types of crypto-assets need to be licensed. Category #1: the token: (i) can be used as a means of payment for goods and/or services (to the extent that the merchants with whom the tokens can be used are not limited to certain persons designated by the issuer); (ii) is exchangeable for any fiat currency; and (iii) is electronically transferable. Category #2: the token both: (i) is exchangeable for Category #1 crypto-assets; and (ii) is electronically transferable.

**Todd W. Beauchamp****Tel: +1 202 637 2294 / Email: todd.beauchamp@lw.com**

Todd Beauchamp is a partner in the Washington, D.C. office of Latham & Watkins and a member of the firm's Financial Institutions Industry Group. He serves as Global Co-Chair of the FinTech Industry Group and leads the Payments & Emerging Financial Services Practice. Mr. Beauchamp represents financial institutions, non-bank financial services companies, as well as technology companies, on a full spectrum of regulatory, transactional, and general corporate matters. He has comprehensive knowledge of emerging payment technologies, including those related to money transmission, virtual currencies, electronic payments, and stored value. Mr. Beauchamp counsels clients on a wide variety of federal, state, and international regulatory issues, as well as legislative developments. Additionally, he represents clients in matters before various state and federal bank regulatory agencies. Mr. Beauchamp advises clients in the structuring and negotiation of corporate transactions and commercial arrangements related to the offering of payments and credit products and services. In addition, he represents clients in the acquisition and sale of financial institutions and non-bank financial services companies, such as state-licensed money transmitters.

**Stephen P. Wink****Tel: +1 212 906 1229 / Email: stephen.wink@lw.com**

Stephen Wink is a partner in the New York office of Latham & Watkins, member of the firm's Financial Institutions and FinTech Industry Groups, and Co-Chair of the firm's Blockchain & Cryptocurrency Task Force. Mr. Wink advises a diverse mix of clients, including broker-dealers, robo-advisors, crowdfunding platforms, cryptocurrency platforms, marketplace lenders, and payments providers on the financial regulatory considerations inherent in their proprietary FinTech transactions. He has in-depth knowledge and broad experience advising financial institutions on regulatory and related matters, gained in part from a decade as general counsel of a full-service investment bank.

**Simon Hawkins****Tel +852 2912 2733 / Email: simon.hawkins@lw.com**

Simon Hawkins is counsel in the Hong Kong office of Latham and Watkins and member of the firm's Financial Institutions and FinTech Industry Groups. Mr. Hawkins' practice focuses on financial regulation, including licensing matters, prime brokerage arrangements, securities dealing, financial market regulations, intermediary and distribution arrangements, product development and structuring, and FinTech. Mr. Hawkins also advises on the regulatory aspects of capital market and M&A deals involving financial institutions, and he has particular expertise in structuring and negotiating bancassurance arrangements.

Latham & Watkins LLP

885 Third Avenue Suite 1000, New York 10022-4834, NY, USA

Tel: +1 212 906 1237 / URL: www.lw.com

Cross-Border Financing of Fintech: A Comparison of Venture and Growth Fintech Financing Trends in Europe and the United States

Jonathan Cardenas
Stanford Law School

Cross-border financing of early-stage technology companies is increasingly recognised as a driver of innovation and national industrial competitiveness.ⁱ In the financial technology (“Fintech”) sector alone, cross-border flows of venture and growth stage investment have skyrocketed to unprecedented levels in recent years, contributing to a proliferation of innovative Fintech start-ups on both sides of the Atlantic. This chapter will provide an overview of recent trends and challenges in venture and growth-stage financing of Fintech start-ups in Europe and the United States (“U.S.”), highlighting the importance of these investments for the transatlantic economy.ⁱⁱ

Global Fintech investment in context

Overall global investment in the Fintech sector amounted to \$55.3B in 2018, spread over a total of 3,251 deals globally, more than doubling the \$26.7B invested in 2017.ⁱⁱⁱ Of this total, venture capital-backed Fintech start-ups raised more than \$39B across 1,707 deals, including 52 “mega” rounds each exceeding \$100M.^{iv} Within this funding landscape emerged 16 Fintech unicorns (those valued at over \$1B) in 2018,^v including Circle (\$3B),^{vi} UiPath (\$3B),^{vii} DevotedHealth (\$1.8B),^{viii} Brex (\$1.1B),^{ix} Dataminr (\$1.2–1.6B),^x Tradeshift (\$1B)^{xi} and Root (\$1B)^{xii} in the U.S., together with Revolut (\$1.7B)^{xiii} and Monzo (\$1.27B)^{xiv} in the United Kingdom (“UK”), among others located elsewhere.^{xv}

Although the U.S. was home to the highest number of Fintech investment transactions in 2018 with over 1,100 deals executed, China accounted for 46% of all Fintech investment volume.^{xvi} The largest Fintech financing transaction in 2018 was that of Hangzhou-based Ant Financial Services Group, which raised a record-breaking \$14B in a financing round co-led by the Singaporean Government’s GIC Private Limited and Temasek Holdings.^{xvii} In the U.S., the total value of Fintech deals increased by 46% in 2018 to \$16.6B, with LendingPoint’s \$600M credit facility financing standing as the largest U.S. Fintech transaction of the year.^{xviii} The total value of Fintech deals also increased in the UK by 50% in 2018 to \$3.9B,^{xix} with the largest transactions including Prodigy Finance’s \$1B financing round,^{xx} Revolut’s \$250M round,^{xxi} Atom Bank’s \$200M round^{xxii} and Monzo’s \$100M round.^{xxiii} In contrast to other regions of the world, however, the total volume of Fintech financing in Europe declined in 2018, yielding a total of approximately \$3.5B.^{xxiv}

Corporate venture capital investment in Fintech

Corporate venture capital investment in Fintech also increased significantly in 2018, with corporate venture capital investors participating in 33% of all Fintech deals globally, amounting to a five-year high.^{xxv} The leading Fintech corporate venture capital investors in 2018 were American Express Ventures, CapitalG (Alphabet’s growth equity investment

fund), Citi Ventures, Goldman Sachs Principal Strategic Investments, Google Ventures, ING Ventures, Munich RE Ventures and Santander InnoVentures.^{xxvi} Among the most significant Fintech corporate venture capital transactions in 2018 were ABN AMRO Digital Impact Fund's investment in solarisBank,^{xxvii} BBVA's investment in Atom Bank,^{xxviii} CapitalG's investment in Robinhood^{xxix} and Morgan Stanley Tactical Value Fund's investment in Dataminr.^{xxx}

In addition to direct corporate venture capital investment in Fintech start-ups, 2018 also saw a growing number of indirect investments by way of incubator and accelerator programmes housed within banks, commonly referred to as "Fintech innovation labs".^{xxxi} Examples include the Barclays Accelerator, BBVA Innovation Labs, Citi Innovation Labs and Innovation at Rabobank.^{xxxii} Corporate venture capital investment in European and U.S. Fintech start-ups is projected to continue to grow in 2019.^{xxxiii}

Early-stage venture financing challenges in Europe

In contrast to the U.S., which has historically been regarded as the strongest market worldwide for the provision of venture capital to early-stage technology companies,^{xxxiv} Europe is widely regarded as a region that faces major obstacles in early-stage venture funding.^{xxxv} The German Private Equity and Venture Capital Association (the *Bundesverband Deutscher Kapitalbeteiligungsgesellschaften* or "BVK"), for example, has recognised that early-stage German technology start-ups face barriers in obtaining domestic venture capital funding due, in part, to the relatively low number of large venture capital funds in Germany combined with a lack of interest from institutional investors in the small German venture capital funds that currently exist.^{xxxvi} In addition, the German venture capital ecosystem is constrained by an overall culture of financial risk aversion that produces an inclination towards debt financing rather than equity financing.^{xxxvii} Similar views have been expressed with respect to the venture capital environment in the European Union ("EU") as a whole by the European Commission and Invest Europe (formerly known as the European Private Equity & Venture Capital Association).^{xxxviii}

European venture financing constraints, which are present across all industries, directly impact Fintech start-ups and are one reason for the relative decline in total volumes of Fintech financing in Europe in 2018. As described in further detail below, various public sector initiatives have been implemented in Europe to stimulate pan-European venture capital investment in early-stage European technology start-ups. Each of these initiatives is likely to increase the amount of capital that is available to early-stage European Fintech start-ups in the future.

Public-private partnership model in German venture capital

The combination of a risk-averse financial culture in Germany^{xxxix} with an overall shortage of large-scale venture capital funds has led to the implementation of the public-private partnership model – traditionally deployed in the financing of public infrastructure projects – in the venture capital sphere. The Bonn-based High-Tech Gründerfonds ("HTGF"), for example, which is Germany's largest seed investor,^{xl} is structured as a public-private partnership venture capital firm. HTGF's investor base includes major public sector institutions, such as the German Federal Ministry for Economic Affairs and Energy, the German state-owned development bank Kreditanstalt für Wiederaufbau ("KfW"), and the Fraunhofer Society for the Advancement of Applied Research ("Fraunhofer-Gesellschaft"), as well as private sector actors, such as BASF, Deutsche Post DHL and Robert Bosch, among others.^{xli} HTGF has invested approximately €892M in more than 500 seed-stage German

technology start-ups,^{xlii} and is considered a significant player in the German Fintech sector. Recent HTGF seed financings in Fintech include Berlin-based insurtech start-up remind.me in May 2018,^{xliii} North Rhine-Westphalia-based digital debt collection start-up troy in September 2018,^{xliiv} Frankfurt-based crypto asset management firm Iconiq Holding in January 2019,^{xliv} and Frankfurt-based blockchain services provider Agora Innovation in February 2019.^{xlvi} While the public-private partnership model has proven to be successful in the German context, the level of funding that it has provided is simply not enough to enable German and European start-ups to compete on a global scale.

EU venture capital fund-of-funds programme

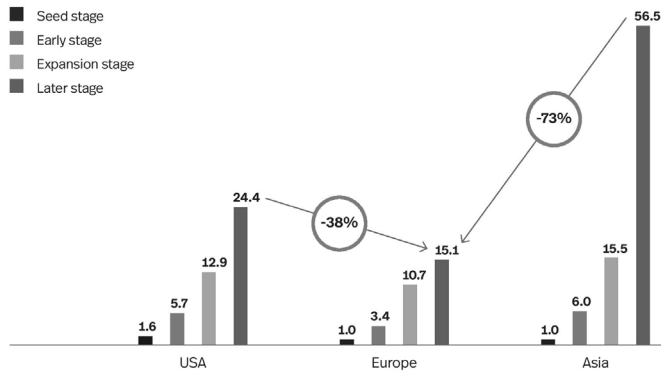
In an effort to “bridge the gap” that exists between small European venture capital funds and large institutional investors,^{xlvii} the European Commission and the European Investment Fund (“EIF”) launched a pan-European venture capital fund-of-funds programme known as VentureEU in April 2018.^{xlviii} Developed under the auspices of the European Commission’s Capital Markets Union Action Plan, VentureEU is expected to stimulate €6.5B of investment in “start-up and scale-up” companies across the EU by way of six fund-of-funds that will invest public and private sector capital in small venture capital funds, each of which is required to focus on investment projects in at least four European jurisdictions.^{xlix} Funding into each of the six VentureEU fund-of-funds consists of an initial “cornerstone” investment of up to €410M from EU institutions, including the European Investment Fund, the Horizon 2020 InnovFin Equity initiative, COSME (the EU programme for the Competitiveness of Enterprises and SMEs), and the European Fund for Strategic Investments, with the remainder provided by private investors in matching amounts.¹

The VentureEU programme has sparked the creation of similar initiatives at the EU Member State level. In March 2019, for example, the EIF and Axis, the wholly-owned venture capital arm of Spanish credit institution Instituto de Crédito Oficial, jointly launched a €40M angel investment fund geared toward Spanish early-stage technology start-ups.^{li} The fund, which forms part of EIF’s European Angels Fund initiative,^{lii} will provide funding to angel investors who invest in the Spanish market. In addition, the EIF and Germany’s Fraunhofer-Gesellschaft established a joint technology transfer fund in February 2019 under the auspices of the European Commission’s EU Finance for Innovators (“InnovFin”) programme.^{liii} This €60M Fraunhofer Tech Transfer Fund will help to commercialise intellectual property generated by researchers at the Fraunhofer-Gesellschaft’s 72 research institutes, with the intent of catalysing spin-offs that will transfer technology “from the laboratory to the economy”.^{liv} The launch of these initiatives is projected to stimulate deeper investment in early-stage technology start-ups across Europe and is likely to provide further impetus for venture capital investment in the European Fintech sector.

Growth equity investment in Fintech

In addition to venture capital financing barriers that exist at the nascent stage of development, European technology start-ups wrestle with financing obstacles at the growth stage, which is commonly referred to as the “turning point” for market entry.^{lv} As the below graph illustrates, Europe trailed behind Asia and the U.S. in 2018 with respect to levels of venture capital invested in both expansion and later-stage start-ups:^{lvi}

Average venture capital investment per company by phase in the startup lifecycle in Q2 2018 [EUR m]



Source: German Private Equity and Venture Capital Association (BVK), Roland Berger, Internet Economy Foundation, CB Insights and PwC. Figures have been rounded.

In recent years, however, an increasing amount of capital has been invested in growth-stage start-ups through growth private equity (“growth equity”) investment vehicles, which attract limited partners that seek exposure to technology start-ups with potentially lower risk profiles than those at earlier stages of development.^{lvii} In 2018, overall growth equity investment reached record levels, with \$66.1B invested across 1,057 deals in the U.S. alone.^{lviii} 2018 also saw the largest ever growth equity fundraise with the close of New York-based Insight Venture Partners’ \$6.3B technology-focused growth equity fund.^{lix} This trend may help to fill at least some of Europe’s growth-stage funding gap.

Defining growth equity

Growth equity (also known as “growth capital” or “expansion capital”) is often referred to as the intersection between venture capital and leveraged buyouts.^{lx} To date, there is no universally accepted definition of growth equity due, in part, to its similarity to other forms of alternative investment. The U.S. National Venture Capital Association (“NVCA”) and its Growth Equity Group have described growth equity as a “critical component” of the venture capital industry, and have defined growth equity investments as those that exhibit some, if not all, of the following characteristics: investors typically acquire a non-controlling minority interest in the company; investments are often unlevered or use only light leverage; the company is founder-owned and/or founder-managed with a proven business model, positive cash flows and rapidly growing revenues; and invested capital is geared towards company expansion and/or shareholder liquidity, with additional financing rounds typically not expected until the growth equity investor’s exit.^{lxi} The European Bank for Reconstruction and Development has defined growth equity in a similar way, but has specifically included mezzanine financing within its definition as a result of private equity investment patterns in the emerging Europe and Central Asia regions, which typically consist of combinations of venture, growth and buyout strategies.^{lxii}

Growth equity investors include, but are not limited to, traditional private equity and venture capital firms that offer growth equity as one of several strategies, specialist growth equity firms, strategic corporate investors, and non-traditional institutional investors, such as pension funds and single family offices, which historically have not invested in emerging

companies. In 2018, the 10 most active growth equity investors were Business Growth Fund, Bpifrance, Foresight Group, Warburg Pincus, Kohlberg Kravis Roberts, The Blackstone Group, CM-CIC Investissement, Caisse de dépôt et placement du Québec, TPG Capital and General Atlantic.^{lxiii} Of the 24 most active growth equity investors in 2018, the majority were concentrated in the U.S., France and the UK, respectively.^{lxiv}

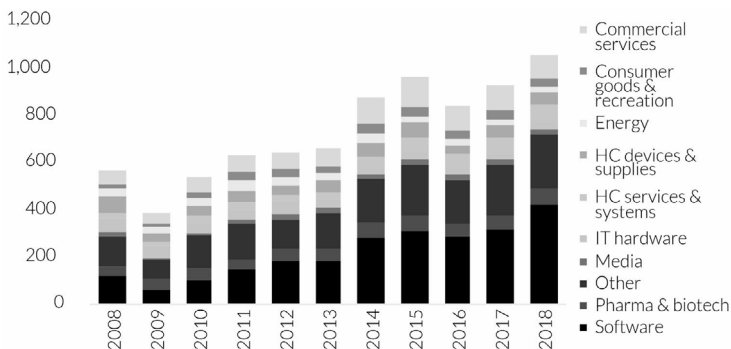
From the company perspective, growth equity investment, in its varying shapes and sizes, fuels later-stage expansion into new product and/or geographic markets, often in preparation for a future merger, acquisition or initial public offering. In contrast to multi-investor early-stage venture financing rounds, growth equity investment may provide the company with the benefit of a higher-stake single investor who can provide strategic business and operational guidance that can translate into greater market share and profitability. This benefit, however, can become a double-edged sword for founders as a result of the growth equity investor's potentially more significant influence over management decisions.

Fintech as a growth equity investment target

From the investor perspective, technology start-ups are considered attractive growth equity investment targets as a result of their perceived revenue stability and high growth potential.^{lxv} Software start-ups in the Fintech sector, in particular, attract strong interest from growth equity investors.^{lxvi} Pitchbook-NVCA Venture Monitor data in the below graph evidences this trend.^{lxvii}

Growth equity deals in software startups increase in 2018

US growth equity deals (#) by industry



Source: Pitchbook-NVCA Venture Monitor (2019)

In the UK alone, growth equity investment in the Fintech sector rose by 57% in 2018 to \$1.6B.^{lxviii} Among the largest UK growth equity investments in Fintech in 2018 were General Atlantic's \$250M investment in lending start-up Greensill Capital^{lxix} and BBVA's £85.4M investment in mobile-banking platform Atom Bank.^{lxx}

The number of growth equity funds that have been formed in Europe has also grown in recent years,^{lxxi} and includes Atlantic Labs' Growth I Fund, Citizen Capital II Fund, Digital+ Partners Digital Growth Fund I and Verdane Capital's ETF III Fund.^{lxxii} Recent examples of European growth equity investments in Fintech include Bridgepoint Capital's lead investment in Kyriba,^{lxxiii} and Vitruvian Partners' lead investments in Deposit Solutions^{lxxiv} and smava.^{lxxv} In the U.S., recent examples of growth equity investments in Fintech include DST Global's lead investment in Chime Bank,^{lxxvi} Edison Partners' lead investment in

YieldStreet,^{lxxvii} Great Hill Partners' lead investment in Mineral Tree^{lxxviii} and Goldman Sachs Principal Strategic Investments' lead investment in Nav Technologies.^{lxxix}

With injections of growth equity, Fintech start-ups can deepen their domestic market share, as well as their international reach. Growth equity investment in UK Fintech start-ups, in particular, has fuelled their ambitions to expand into the U.S. market. One such example is UK-based small and medium-sized enterprise lending platform Oak North, which plans to launch in the U.S. in 2019 following a \$440M growth equity investment from Softbank Vision Fund and the Clermont Group.^{lxxx}

Growth equity is projected to continue its upward trend as an investment strategy of choice for later-stage investors in the Fintech sector. With higher levels of growth equity invested in promising Fintech start-ups on both sides of the Atlantic, the transatlantic investment relationship in the Fintech sector is likely to deepen and the strength of the European and U.S. Fintech ecosystems is likely to augment.

Conclusion

With record-breaking levels of Fintech investment in 2018, the European and U.S. Fintech ecosystems continue to grow at remarkable speeds. Notwithstanding the early- and growth-stage financing obstacles that currently limit the scale of the European Fintech financing market, cross-border Fintech investment between the EU and U.S. continues to drive innovation and stimulate economic growth on both sides of the Atlantic. With a rapidly evolving transatlantic Fintech market, cross-border Fintech M&A and IPO activity is likely on the way. Attorneys on both sides of the Atlantic should therefore pay close attention to developments in this space.

Acknowledgment

The author would like to thank the Transatlantic Technology Law Forum at Stanford Law School for its encouragement in the undertaking of comparative and international academic research on venture capital financing of Fintech.

Disclaimer

The views and opinions expressed in this chapter are those of the author alone, and do not necessarily reflect the views of Stanford University, the University of Vienna, the American Bar Association or Crowell & Moring LLP. The material in this chapter has been prepared for informational purposes only and is not intended to serve as legal or investment advice.

* * *

Endnotes

- i. For an academic perspective, see Bradley, W. *et al.*, *Cross-Border Venture Capital Investments: What is the Role of Public Policy?*, University of Oxford Saïd Business School WP 2019-02, European Corporate Governance Institute (ECGI) – Finance Working Paper No. 591/2019 (January 2019). Available at: <https://www.law.ox.ac.uk/business-law-blog/blog/2019/02/cross-border-venture-capital-investments-what-role-public-policy>. See also Andrea Schertler, A. and Tykvová, T., *What Lures Cross-Border Venture Capital Inflows?*, Leibniz-Zentrum für Europäische Wirtschaftsforschung (ZEW) Discussion Paper No. 10-001 (January 2010).

- Available at: <ftp://ftp.zew.de/pub/zew-docs/dp/dp10001.pdf>. For a German industry perspective, see German Private Equity and Venture Capital Association (BVK) *et al.*, *Venture Capital: Fueling innovation and economic growth* (June 2018). Available at: https://www.bvkap.de/sites/default/files/publication/rb_pub_18_019_cop_ief_bvk_online_en_with_publication_date.pdf. For a European industry perspective, see Investment & Pensions Europe (IPE) International Publishers Ltd. (2019), *Venture capital: Venturing further in Europe* (February 2019). Available at: <https://www.ipe.com/investment/asset-class-reports/private-equity/venture-capital-venturing-further-in-europe/10029270.article>. See also Invest Europe, *Innovation boosts Europe's lead as global investment destination* (5 November 2018). Available at: <https://www.investeurope.eu/news-opinion/newsroom/press-releases/2018-global-investment-decision-makers-survey/>.
- ii. See European Commission Directorate-General for Research and Innovation, *Study on Transatlantic Dynamics of New High Growth Innovative Firms* (2016). Available at: <https://publications.europa.eu/en/publication-detail/-/publication/a9b6ac9d-31cc-11e7-9412-01aa75ed71a1/language-en>. See also The German Marshall Fund of the United States, *What do High-Growth Firms in the United States and Europe Teach Policymakers?* (August 2012). Available at: <http://www.gmfus.org/file/2729/download>. For a high-level overview of the economic value of venture capital, see Strebulaev, I. and Gornall, W., *The Economic Impact of Venture Capital: Evidence from Public Companies*, Stanford University Graduate School of Business Research Paper No. 15-55 (2015). Available at: <https://www.gsb.stanford.edu/faculty-research/working-papers/economic-impact-venture-capital-evidence-public-companies>.
 - iii. Accenture, *Global Fintech Investments Surged in 2018 with Investments in China Taking the Lead, Accenture Analysis Finds; UK Gains Sharply Despite Brexit Doubts* (25 February 2019). Available at: <https://newsroom.accenture.com/news/global-fintech-investments-surged-in-2018-with-investments-in-china-taking-the-lead-accenture-analysis-finds-uk-gains-sharply-despite-brexit-doubts.htm>.
 - iv. CB Insights, *Fintech Trends to Watch in 2019* (February 2019). Available at: <https://www.cbinsights.com/research/report/Fintech-trends-2019/>. See also CB Insights, *These Are The Most Active Fintech Investors in 2018* (18 February 2019). Available at: <https://www.cbinsights.com/research/top-Fintech-investors-2018/>.
 - v. CB Insights, *Fintech Trends to Watch in 2019* (February 2019).
 - vi. Fortune, *Cryptocurrency Exchange Circle Valued at Nearly \$3 Billion After Poloniex Deal* (15 May 2018). Available at: <http://fortune.com/2018/05/15/cryptocurrency-exchange-circle-bitmain-value/>.
 - vii. TechCrunch, *'Software robot' startup UiPath expands Series C to \$265M at a \$3B valuation* (14 November 2018). Available at: <https://techcrunch.com/2018/11/14/software-robot-startup-uipath-expands-series-c-to-265m-at-a-3b-valuation/>.
 - viii. CNBC, *Devoted Health, a start-up selling health insurance to seniors, is worth \$1.8 billion* (17 October 2018). Available at: <https://www.cnbc.com/2018/10/17/devoted-health-is-valued-at-1point8-billion-in-funding-led-by-andressen.html>.
 - ix. Forbes, *Brex Has Amassed A Valuation Of \$1.1 Billion In Under Two Years* (5 October 2018). Available at: <https://www.forbes.com/sites/donnaufuscaldo/2018/10/05/brex-has-amassed-a-valuation-of-1-1-billion-in-under-two-years/#15425bbd65a1>.

- x. The Wall Street Journal, *Morgan Stanley Leading Dataminr Round at \$1.2 Billion Pre-Money* (6 June 2018). Available at: <https://www.wsj.com/articles/morgan-stanley-leading-dataminr-round-at-1-2b-pre-money-1528284601>.
- xi. Bloomberg, *Tradeshift Valuation Hits \$1.1 Billion After Pre-IPO Fundraising* (29 May 2018). Available at: <https://www.bloomberg.com/news/articles/2018-05-29/goldman-lead-250-million-funding-round-for-tradeshift>.
- xii. TechCrunch, *A new unicorn is born: Root Insurance raises \$100 million for a \$1 billion valuation* (22 August 2018). Available at: <https://techcrunch.com/2018/08/22/a-new-unicorn-is-born-root-insurance-raises-100-million-for-a-1-billion-valuation/>.
- xiii. CNBC, *Revolut becomes latest fintech unicorn after \$250 million funding gives it a \$1.7 billion valuation* (26 April 2018). Available at: <https://www.cnbc.com/2018/04/26/revolut-raises-250-million-in-funding-at-1-point-7-billion-valuation.html>. See also Reuters, *Revolut becomes Britain's first digital bank unicorn* (26 April 2018). Available at: <https://www.reuters.com/article/us-fintech-revolut-funding/revolut-becomes-britains-first-digital-bank-unicorn-idUSKBN1HX0MZ>.
- xiv. TechCrunch, *Monzo, the UK challenger bank, raises £85M Series E at a £1B pre-money valuation* (30 October 2018). Available at: <https://techcrunch.com/2018/10/30/monzocorn/>.
- xv. CB Insights, *Fintech Trends to Watch in 2019* (February 2019).
- xvi. Accenture (25 February 2019).
- xvii. Wall Street Journal, *Jack Ma's Ant Financial Valued Around \$150 Billion After Funding Round* (7 June 2018). Available at: <https://www.wsj.com/articles/jack-mas-ant-financial-raises-14-billion-1528428455>. See also Accenture (25 February 2019).
- xviii. Accenture (25 February 2019).
- xix. *Id.*
- xx. Forbes, *Cross-Border Student Loan Lender Prodigy Finance Raises \$1B In Debt Financing* (24 September 2018). Available at: <https://www.forbes.com/sites/donnaufuscaldo/2018/09/24/cross-border-student-loan-lender-prodigy-finance-raises-1b-in-debt-financing/>. See also Prodigy Finance, *US\$1 billion in debt financing supports accelerated international student growth* (24 September 2018). Available at: <https://prodigyfinance.com/resources/blog/1-billion-debt-financing-2018>.
- xxi. CNBC, *Revolut becomes latest fintech unicorn after \$250 million funding gives it a \$1.7 billion valuation* (26 April 2018). Available at: <https://www.cnbc.com/2018/04/26/revolut-raises-250-million-in-funding-at-1-point-7-billion-valuation.html>.
- xxii. Financial Times, *Atom Bank in £149m capital raising* (7 March 2018). Available at: <https://www.ft.com/content/9dd3f234-21e3-11e8-add1-0e8958b189ea>. See also Finextra, *BBVA raises Atom Bank stake to 39% as part of £149 million funding round* (7 March 2018). Available at: <https://www.finextra.com/newsarticle/31778/bbva-raises-atom-bank-stake-to-39-as-part-of-149-million-funding-round>.
- xxiii. TechCrunch, *Monzo, the UK challenger bank, raises £85M Series E at a £1B pre-money valuation* (30 October 2018). Available at: <https://techcrunch.com/2018/10/30/monzocorn/>. See also The Telegraph, *Monzo raises £85m to become UK's latest tech 'unicorn'* (31 October 2018). Available at: <https://www.telegraph.co.uk/technology/2018/10/31/monzo-raises-85m-become-uks-latest-tech-unicorn/>.

- xxiv. CB Insights, *Fintech Trends to Watch in 2019* (February 2019). See also Accenture (25 February 2019).
- xxv. CB Insights, *Fintech Trends to Watch in 2019* (February 2019).
- xxvi. Financial Technology Partners, *Annual 2018 Fintech Almanac: Financing & M&A Statistics* (February 2019). Available at: <https://www.ftpartners.com/Fintech-research/almanac>.
- xxvii. ABN AMRO, *ABN AMRO Digital Impact Fund invests in German fintech solarisBank* (8 March 2018). Available at: <https://www.abnamro.com/en/newsroom/press-releases/2018/abn-amro-digital-impact-fund-invests-in-german-fintech-solarisbank.html>.
- xxviii. BBVA, *BBVA backs UK banking disruptor Atom with further investment* (7 March 2018). Available at: <https://www.bbva.com/en/bbva-backs-uk-banking-disruptor-atom-further-investment/>.
- xxix. Robinhood Blog, *Robinhood Raises \$363 Million to Expand Product Lineup* (10 May 2018). Available at: <https://blog.robinhood.com/news/2018/5/9/robinhood-raises-363-million-to-expand-product-lineup>.
- xxx. New York Business Journal, *This week in NYC funding news: The top VC rounds of 2018* (28 December 2018). Available at: <https://www.bizjournals.com/newyork/news/2018/12/28/this-week-nyc-funding-news-the-top-vc-rounds-2018.html>.
- xxxi. CB Insights, *30 Corporate Innovation Labs in Finance* (2018). Available at: <https://www.cbinsights.com/research/report/finance-corporate-innovation-labs/>.
- xxxii. *Id.*
- xxxiii. CB Insights, *The 2018 Global Corporate Venture Capital Report* (28 March 2019). Available at: <https://www.cbinsights.com/research/report/corporate-venture-capital-trends-2018/>. See also The American Banker, *Why Venture Capitalists Love Fintechs* (10 February 2019). Available at: <https://www.americanbanker.com/list/why-venture-capitalists-love-fintechs>.
- xxxiv. See Kaplan, S. and Lerner, J., *It Ain't Broke: The Past, Present, and Future of Venture Capital*, *Journal of Applied Corporate Finance*, Vol. 22, No. 2 (Spring 2010). Available at: <http://www.people.hbs.edu/jlerner/kaplanlerner.jacf.pdf>.
- xxxv. Financial Times, *European Venture Capital Groups Struggle to Attract Investors* (7 February 2008). Available at: <https://www.ft.com/content/845f5cb0-0c19-11e8-839d-41ca06376bf2>. See also Bloomberg, *Why Can't Europe Do Tech* (15 August 2018). Available at: <https://www.bloomberg.com/news/features/2018-08-16/inside-europe-s-struggle-to-build-a-truly-global-tech-giant>.
- xxxvi. German Private Equity and Venture Capital Association (BVK) *et al.* (June 2018).
- xxxvii. German Private Equity and Venture Capital Association (BVK) *et al.* (June 2018).
- xxxviii. European Commission, *VentureEU: €2.1 billion to boost venture capital investment in Europe's innovative start-ups* (10 April 2018). Available at: http://europa.eu/rapid/press-release_IP-18-2763_en.pdf. See also Invest Europe, *EU venture capital programme a 'great step forward', says Invest Europe* (10 April 2018). Available at: <https://www.investeurope.eu/news-opinion/newsroom/press-releases/vc-fof/>.
- xxxix. See Quartz, *Germans don't do tech startups — more access to capital might change that* (30 September 2018). Available at: <https://qz.com/1404647/germans-dont-do-tech-startups-more-access-to-capital-might-change-that/>. See also Maria Ferreira,

- Cross-country differences in risk attitudes towards financial investment* (21 September 2018). Available at: <https://voxeu.org/article/cross-country-differences-risk-attitudes-towards-financial-investment>.
- xl. PitchBook, *The top 11 VC investors in German startups* (14 June 2018). Available at: <https://pitchbook.com/news/articles/the-top-11-vc-investors-in-german-startups>.
- xli. High-Tech Gründerfonds, *A powerful motor for innovation and the economy: High-Tech Gründerfonds makes its 500th investment* (28 June 2018). Available at: <https://high-tech-gruenderfonds.de/en/a-powerful-motor-for-innovation-and-the-economy-high-tech-gruenderfonds-makes-its-500th-investment/>.
- xlii. High-Tech Gründerfonds, *Coinlend receives HTGF seed funding for its AI-based lending platform tailored to the cryptocurrency market* (27 March 2019). Available at: <https://high-tech-gruenderfonds.de/en/coinlend-receives-htgf-seed-funding-for-its-ai-based-lending-platform-tailored-to-the-cryptocurrency-market/>. See also EU-Start-ups.com, *High-Tech Gründerfonds makes and celebrates its 500th investment (Sponsored)* (18 June 2018). Available at: <https://www.eu-startups.com/2018/06/high-tech-gruenderfonds-makes-and-celebrates-its-500th-investment-sponsored/>.
- xliii. High-Tech Gründerfonds, *Berlin-based Fintech start-up remind.me secures seed financing* (24 May 2018). Available at: <https://high-tech-gruenderfonds.de/en/berlin-based-fintech-start-up-remind-me-secures-seed-financing/>.
- xliv. High-Tech Gründerfonds, *New HTGF Fintech investment troy revolutionizes the debt collection process and combines machine learning with friendliness* (3 September 2018). Available at: <https://high-tech-gruenderfonds.de/en/new-htgf-fintech-investment-troy-revolutionizes-the-debt-collection-process-and-combines-machine-learning-with-friendliness/>.
- xlv. High-Tech Gründerfonds, *Iconiq Holding closes a seven-figure financing round as FinLab increases its stake and Germany's largest VC, High-Tech Gründerfonds, invests* (22 January 2019). Available at: <https://high-tech-gruenderfonds.de/en/iconiq-holding-closes-a-seven-figure-financing-round-as-finlab-increases-its-stake-and-germanys-largest-vc-high-tech-gruenderfonds-invests/>.
- xlvi. High-Tech Gründerfonds, *Frankfurt blockchain start-up Agora Innovation secures high six-figure investment from High-Tech Gründerfonds* (25 February 2019). Available at: <https://high-tech-gruenderfonds.de/en/frankfurt-blockchain-start-up-agora-innovation-secures-high-six-figure-investment-from-high-tech-gruenderfonds/>.
- xlvii. European Commission, *VentureEU: Pan-European Venture Capital Funds-of-Funds Programme: Frequently asked questions* (10 April 2018). Available at: https://europa.eu/rapid/press-release_MEMO-18-2764_en.pdf.
- xlviii. European Commission, *VentureEU: €2.1 billion to boost venture capital investment in Europe's innovative start-ups* (10 April 2018).
- xlix. European Commission, *Start-ups and Scale-Ups: The Wide EU Ecosystem* (2018). Available at: <http://europa.eu/rapid/attachment/IP-18-2763/en/Factsheet%20VentureEU-EU%20ecosystem.pdf>.
- i. European Commission, *VentureEU: €2.1 billion to boost venture capital investment in Europe's innovative start-ups* (10 April 2018).
- ii. The European Investment Fund, *European Investment Fund (EIB Group) and Axis launch new investment fund for financing innovative firms in Spain* (21 March 2019).

- Available at: https://www.eif.org/what_we_do/equity/news/2019/axis-investment-fund-spain.htm.
- lii. European Investment Fund, *European Angels Fund (EAF)*. Available at: https://www.eif.org/what_we_do/equity/eaf/index.htm.
 - liii. European Investment Fund, *European Investment Fund and Fraunhofer join forces to establish joint technology transfer fund in Germany* (26 February 2019). Available at: https://www.eif.org/what_we_do/equity/news/2019/fraunhofer-efsi-innovfin.htm. See also European Investment Fund, *InnovFin – EU Finance for innovators*. Available at: <https://www.eib.org/en/products/blending/innovfin/index.htm>.
 - liv. European Investment Fund (26 February 2019).
 - lv. German Private Equity and Venture Capital Association (BVK) *et al.* (June 2018). Available at: https://www.bvkap.de/sites/default/files/publication/rb_pub_18_019_cop_ief_bvk_online_en_with_publication_date.pdf.
 - lvi. *Id.*
 - lvii. Preqin, *Growth Equity: Return Expectations and Prospects in Growth PE Investing* (15 November 2017).
 - lviii. PitchBook, *4Q 2018 Pitchbook–NVCA Venture Monitor* (2019). Available at: <https://pitchbook.com/news/reports/4q-2018-pitchbook-nvca-venture-monitor>.
 - lix. PitchBook, *3Q 2018 US PE Breakdown* (2018). Available at: <https://pitchbook.com/news/reports/3q-2018-us-pe-breakdown>. Insight Venture Partners, Software Investor Insight Venture Partners Closes \$6.3 Billion Fund X (19 July 2018). Available at: <https://www.insightpartners.com/about-us/news-press/software-investor-insight-venture-partners-closes-6-3-billion-fund-x/>.
 - lx. PitchBook, *3Q 2018 US PE Breakdown* (2018).
 - lxi. National Venture Capital Association Growth Equity Group, *Defining Growth Equity Investments*. Available at: <https://nvca.org/growth-equity-group/>.
 - lxii. European Bank for Reconstruction and Development, *EBRD Transition Report 2015-16* (2015). Available at: <https://www.ebrd.com/news/publications/transition-report/ebd-transition-report-201516.html>.
 - lxiii. PitchBook, *2018 Annual Global League Tables* (31 January 2019). Available at: <https://pitchbook.com/news/reports/2018-annual-global-league-tables>.
 - lxiv. *Id.*
 - lxv. PitchBook, *1Q 2018 Pitchbook–NVCA Venture Monitor* (9 April 2018). Available at: <https://pitchbook.com/news/reports/1q-2018-pitchbook-nvca-venture-monitor>.
 - lxvi. American Banker, *Money Keeps Flowing to Fintechs* (14 March 2019). Available at: <https://www.americanbanker.com/list/money-keeps-flowing-to-fintechs>.
 - lxvii. PitchBook, *4Q 2018 Pitchbook–NVCA Venture Monitor* (2019).
 - lxviii. Innovate Finance, *2018 Fintech VC Investment Landscape* (2019). Available at: <https://cdn2.hubspot.net/hubfs/5169784/Innovate-Finance-2018-FinTech-VC-Investment-Landscape.pdf>.
 - lxix. General Atlantic, *General Atlantic Announces Strategic Investment in Greensill* (16 July 2018). Available at: <https://www.generalatlantic.com/media-article/general-atlantic-announces-strategic-investment-in-greensill/>. See also The Wall Street Journal, *General Atlantic Invests \$250 Million in Lending Startup Greensill* (16

- July 2018). Available at: <https://www.wsj.com/articles/general-atlantic-invests-250-million-in-lending-startup-greensill-1531713660>.
- lxx. BBVA, *BBVA backs UK banking disruptor Atom with further investment* (7 March 2018). Available at: <https://www.bbva.com/en/bbva-backs-uk-banking-disruptor-atom-further-investment/>. See also BBVA, *BBVA completes £85.4m investment into UK Digital bank Atom, increasing stake to 39%* (1 June 2018). Available at: <https://www.bbva.com/en/bbva-completes-85-4m-investment-uk-digital-bank-atom-increasing-stake-39/>.
- lxxi. Invest Europe, *2017 European Private Equity Activity*, 2 May 2018. Available at: <https://www.investeurope.eu/media/711867/invest-europe-2017-european-private-equity-activity.pdf>. See also Prequin, *The Rise Of Venture And Growth Capital In Europe* (9 August 2018). Available at: <https://www.valuewalk.com/2018/08/rise-venture-growth-capital-europe/>.
- lxxii. European Investment Fund, *Signed Equity deals as of 30/06/2018* (2018). Available at: https://www.eif.org/what_we_do/equity/eif-equity-portfolio.pdf.
- lxxiii. Bridgepoint, *Bridgepoint to acquire Kyriba* (28 March 2019). Available at: <http://www.bridgepoint.eu/en/news/press-releases/2019/bridgepoint-to-acquire-kyriba/>. See also San Diego Business Journal, *Kyriba to Become San Diego's Next Unicorn with \$160M Investment* (27 March 2019). Available at: <https://www.sdbj.com/news/2019/mar/27/kyriba-become-san-diegos-next-unicorn-160m-investm/>.
- lxxiv. Business Insider, *A German fintech startup backed by Peter Thiel has raised \$100 million* (16 August 2018). Available at: <http://www.businessinsider.com/german-fintech-deposit-solutions-raises-100-million-2018-8>. See also Financial Partners, *FT Partners Advises Vitruvian on its Investment in Deposit Solutions* (15 August 2018). Available at: <https://www.ftpartners.com/transactions/vitruvian>.
- lxxv. smava, *smava receives \$65 million investment led by Vitruvian Partners* (9 January 2018). Available at: <https://www.smava.de/presse/pressemitteilungen/smava-receives-65-million-investment/>. See also Reuters, *Vitruvian puts German fintech Smava up for sale: sources* (13 February 2019). Available at: <https://www.reuters.com/article/us-vitruvian-smava-divestiture-idUSKCN1Q2194>.
- lxxvi. Bloomberg, *Online Bank Chime Is Close to New Funding at a \$1.5 Billion Value* (5 February 2019). Available at: <https://www.bloomberg.com/news/articles/2019-02-05/online-bank-chime-is-said-to-near-funding-at-1-5-billion-value>. See also Forbes, *Chime Raises \$200 Million At \$1.5 Billion Valuation* (5 March 2019). Available at: <https://www.forbes.com/sites/donnafuscaldo/2019/03/05/chime-raises-200-million-at-1-5-billion-valuation/>.
- lxxvii. Edison Partners, *Edison Partners Leads \$62 Million Investment in YieldStreet* (26 February 2019). Available at: <https://www.edisonpartners.com/blog/yieldstreet-investment>. See also Forbes, *YieldStreet Raises \$62M To Bring Alternative Investing To The Masses* (26 February 2019). Available at: <https://www.forbes.com/sites/donnafuscaldo/2019/02/26/yieldstreet-raises-62m-to-bring-alternative-investing-to-the-masses/>.
- lxxviii. Great Hill Partners, *MineralTree Closes \$50 Million Growth Financing* (28 March 2019). Available at: <https://www.greathillpartners.com/mineraltree-closes-50-million-growth-financing/>. See also Boston Business Journal, *Cambridge fintech firm MineralTree closes \$50M round led by Great Hill Partners* (27 March 2019).

- Available at: <https://www.bizjournals.com/boston/news/2019/03/27/cambridge-fintech-firm-mineraltree-closes-50m.html>.
- lxxix. Reuters, *Goldman Sachs, Point72 and others invest \$44 million in business credit startup Nav* (11 February 2019). Available at: <https://www.reuters.com/article/us-nav-investment-goldman-sachs-idUSKCN1Q01BJ>.
- lxxx. CNBC, *SoftBank leads \$440 million investment in UK fintech OakNorth, valuing it at \$2.8 billion* (8 February 2019). Available at: <https://uk.finance.yahoo.com/news/softbank-apos-vision-fund-pumps-100413059.html>. See also Finextra, *OakNorth raises \$440 million for US expansion* (8 February 2019). Available at: <https://www.finextra.com/newsarticle/33346/oaknorth-raises-440-million-for-us-expansion>.

**Jonathan Cardenas****Tel: +1 650 723 2465**

Jonathan Cardenas is a Fellow with the Transatlantic Technology Law Forum at Stanford Law School. He is a former Visiting Fellow at Yale Law School's Information Society Project, and a former visiting researcher at the Swiss Federal Institute of Technology ("ETH Zürich") Center for Law & Economics. He serves as Founding Chair of the Financial Services Technology Joint Subcommittee within the Commercial Finance Committee and Private Equity & Venture Capital Committee of the American Bar Association's Business Law Section.

Jonathan received his J.D. from New York University School of Law, where he was a Jacobson Leadership Program in Law & Business Scholar, and where he served as a Managing Editor of the NYU Journal of Law & Business. He received an M.Phil. in International Relations from the University of Cambridge, and a B.A. in Political Science, *summa cum laude*, from the University of Pennsylvania.

Jonathan is admitted as an attorney in the District of Columbia, the State of Florida, and the State of New York. He practises law as a corporate associate with Crowell & Moring in Washington, D.C.

Stanford Law School

559 Nathan Abbott Way, Stanford, CA 94305, USA
Tel: +1 650 723 2465 / URL: www.law.stanford.edu

Australia

Peter Reeves
Gilbert + Tobin

Approaches and developments

Australia has seen a continued proliferation of active fintech businesses, with payments, investment and data emerging as the key sectors for disruption.

Businesses have been exploring new automated service methods including the use of robo-advisors for distributing financial advice in more cost-effective ways. There has been sustained attention on blockchain and distributed ledger technology (DLT) to the extent that fintechs have begun formalising use cases for DLT, such as managing supply chains, making cross-border payments, trading derivatives, managing assets and managing digital currency exchanges. The Australian Securities Exchange (ASX), Australia's primary securities exchange, is currently in the process of rolling out a DLT-based replacement for its clearing and settlement process. Similarly, initial coin offerings (ICOs) have become an alternative method of funding for blockchain or cryptocurrency-related projects.

As discussed below under "Regulatory bodies", Australian regulators have generally been receptive to the growth of the Australian fintech ecosystem and there has been considerable discussion around the opportunities, risks and challenges that have arisen for market participants, customers and regulators. Australian policy-makers and bodies continue to make regulatory and legislative developments to ensure the scope of emerging services is adequately captured within the existing financial services framework. This has included increased technology-neutral or fintech-specific regulatory guidance to assist businesses in understanding their obligations, amended legislation to bring fintech services providers within the remit of existing regimes, and the introduction of new legislation to provide greater consumer protection.

Following the delivery of the Final Report of the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry (Royal Commission), regulatory focus has pivoted to make consumer protection the utmost priority for incumbent financial institutions. Highlighting the industry's sales over service-related misconduct, the Royal Commission's findings have demonstrated the need for industry-wide change to the culture and governance of financial services providers to prioritise the interests of consumers. In the future, regulators are likely to take a more stringent approach to enforcement. For example, the Australian Securities and Investments Commission (ASIC), which has announced a new "why not litigate" regulatory stance, has been empowered with additional penalty provisions under the *Treasury Laws Amendment (Strengthening Corporate and Financial Sector Penalties) Act 2018* (Cth) to provide greater deterrence value against misconduct in the financial services sector. This presents an opportunity for fintechs, which are historically focused on delivering customer-centric outcomes and are often better placed to respond quickly to regulatory change.

The implementation of the new national Consumer Data Right (CDR) framework is anticipated to address many of the issues identified in the Royal Commission, and have a profound effect on the financial services industry by encouraging customers to switch service providers and open the market to new fintech businesses. The CDR framework will first be applied to the banking sector under the “Open Banking” regime, enabling consumers to exercise greater access and control over their banking data. The open banking regime is expected to commence in February 2020.

There have been a number of relevant legislative changes in Australia (see “Fintech offering in Australia” below). In April 2019, the Treasury Laws Amendment (Design and Distribution Obligations and Product Intervention Powers) Bill 2019 received royal assent, which introduces a design and distribution obligation for financial services firms as well as a product intervention power for ASIC. The new obligations will bring accountability for issuers and distributors to design, market and distribute financial and credit products that meet customer needs. To be phased in over two years, the new regime will require product issuers to ensure products are targeted and offered to the right customers and enable ASIC to intervene when inappropriate products are distributed. More than ever, it will be important for financial service providers, including fintechs, to consider the suitability of products and disclosure documents for their own unique customer base.

Fintech offering in Australia

Fintech businesses have been disrupting the Australian banking, investment and wealth management, payments, advisory, trading and fundraising sectors through offers of alternatives to the relatively concentrated traditional providers of these financial services. These alternative offers generally focus on providing financial services in a way that prioritises customer experience and outcomes, utilises technology solutions such as apps and smart devices in the delivery of financial services, or disintermediates the provision of financial services.

Fintech businesses must comply with all existing laws and regulations for financial services and consumer credit activities in Australia. The Australian Government has taken steps to alleviate the regulatory burden on fintechs looking to test the Australian market prior to a full product or service launch. See “Key regulations and regulatory approaches” below for further discussion.

Regulatory guidance has also been updated to address the fintech sector. For example, ASIC has released specific guidance clarifying the licensing, conduct and disclosure obligations that apply to the provision of digital financial product advice. This includes requiring nomination of a person within the business who understands and will be responsible for the ongoing monitoring of the algorithms used to produce any advice provided.

ASIC has clarified how Australian financial services laws may apply to ICOs as an alternative funding mechanism. In summary, the legal status of an ICO depends on the structure, operation and the rights attached to the tokens offered. Tokens offered during the ICO may trigger licensing, registration and disclosure requirements, if the tokens are financial products (e.g., interests in managed investment schemes, securities, derivatives or non-cash payment facilities). Cryptocurrency-related funding rounds are increasingly being considered an offering of a financial product and there is a growing trend for offerors to pre-emptively step into the regulatory framework by means of a security token offering (STO).

Blockchain technology continues to capture the attention of established businesses. In the past couple of years, Australia has witnessed the application of DLT in solutions across a

broad range of financial market operators, financial institutions, financial service providers and fintechs which has prompted new regulation. In 2018, ASIC introduced a two-tiered market licensing regime for financial market operators and updated its corresponding regulatory guidance. Specifically, the guidance reflects a risk-based assessment that will be undertaken, which is consistent with the approach taken internationally to the administration of market licensing. Under the revised Australian market licence (**AML**) regime, market venues can be designated as being either Tier 1 or Tier 2, depending on their nature, size, complexity and the risk they pose to the financial system, investor confidence and trust. While Tier 1 market venues are, or are expected to become, significant to the efficiency and integrity of (and confidence in) the Australian financial system, Tier 2 licences will be able to facilitate a variety of market venues and will have reduced obligations to accommodate new and specialised market platforms. The tiered market regime is expected to impact, amongst others, market operators and operators of market-like venues, as well as platforms seeking to offer secondary trading.

The Australian banking sector is highly regulated with stringent licensing, conduct (including reporting) and regulatory capital requirements which act as significant hurdles for new businesses entering the market. Any entity that conducts any “banking business”, such as taking deposits (other than as part-payment for identified goods or services) or making advances of money, must be licensed as an authorised deposit-taking institution (**ADI**). Recently, the Australian Prudential Regulation Authority (**APRA**) released a new Restricted ADI framework which allows new businesses entering the banking industry to conduct a limited range of banking activities for two years while they build their capabilities and resources. After such time, they must either transition to a full ADI licence or exit the industry. In January 2019, the first Restricted ADI licensee was granted a full ADI licence which allows it to operate as an ADI without restrictions under the *Banking Act 1959* (Cth). The licensee is a “neobank”, which is a wholly digital quasi-bank that intends to provide full banking services to customers via a solely mobile platform. These types of entities use an internet or mobile platform to interact with customers and offer a different user experience from a traditional bank.

Fintech businesses will generally have obligations under the *Anti-money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (**AML/CTF Act**) and *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No.1)* (**AML/CTF Rules**). The AML/CTF Act applies to entities that provide “designated services” with an Australian connection. In 2018, the AML/CTF Act was amended to capture digital currency exchange providers within the scope of the regime by registering and enrolling with the Australian Transaction Reports and Analysis Centre (**AUSTRAC**). Registered exchanges are required to implement know-your-customer processes to adequately verify the identity of their customers, adopt and maintain an AML/CTF programme as well as meet ongoing obligations to monitor and report suspicious and large transactions. The money-laundering risk associated with social media platforms is likely to become a focus for Australian regulators such as AUSTRAC. In early 2019, the Asia/Pacific Group on Money Laundering published a report on the capacity for money laundering and terrorism financing through the abuse of social media services, particularly due to the anonymity of users and speed of payment flows. The report provided measures for authorities to overcome detection, investigation and prosecution challenges. AUSTRAC has not yet responded to the report; however, we would expect to see consideration of the risks incorporated in any future proposed reforms to the AML/CTF Act.

Regulatory and insurance technology

The rising cost of compliance has prompted many companies using artificial intelligence (AI), customer due-diligence (e.g., “know-your-customer”) and data breach monitoring (e.g., “know-your-data”) technologies to invest in regulatory technology, or regtech. ASIC has indicated the benefits of regtech to provide better outcomes for consumers and has hosted annual forums to provide an environment for collaborative information sharing between businesses and to promote stakeholder engagement. It has also been reported that ASIC has actively encouraged incumbent financial institutions to partner with fintechs to harness regtech to automate regulatory reporting, manage compliance and ensure clarity to how regulation is interpreted.

ASIC has announced three events to be held over 2019 which are designed to further promote regtech adoption with respect to monitoring and analysing financial advertising, detecting problematic financial advice, and highlighting the use case for voice analytics and voice-to-text technology for regulatory activity. The industry has called for ASIC to design regulation and guidance in formats aiding regtech applications, to provide best practice-style guidance on compliance and the use of algorithms in the provision of financial services, and to harmonise industry standards with respect to risk management, compliance and reporting obligations. AUSTRAC has also hosted a regtech showcase, inviting demonstrations from providers of innovative solutions to regulatory challenges presented in the AML/CTF space. Investments in insurance technology in Australia have increased, with companies and fintechs focusing on forging cross-sector alliances in order to embed their offerings into alternative value propositions. Insurance technology has the potential to disrupt individual sections of the insurance value chain, augment the existing processes of underwriting risk and predicting loss, and improve the existing capabilities of insurers, reinsurers, intermediaries and service providers. The increase in partnerships and alliances between insurance fintechs and incumbents with established customer bases will be effective for insurance start-ups to fuel expansion.

There have not been any specific changes to legislation or regulation due to regtech or insurance technology; however, this may change in the future as uptake increases and becomes more mainstream.

Regulatory bodies

Australian has a twin peaks model of regulation with respect to financial services:

1. ASIC is Australia’s primary corporate, markets, financial services and consumer credit regulator. It is responsible for regulating consumer protection and maintaining market integrity within the financial system. ASIC supervises the conduct and regulation of Australian companies, financial markets, and financial service and consumer credit providers.
2. APRA is concerned with maintaining the safety and soundness of financial institutions, promoting financial stability in Australia and is tasked with protecting the interests of depositors, policy-holders and superannuation fund members. APRA oversees ADIs (e.g., banks, building societies and credit unions), general and life insurers, friendly societies, reinsurers and superannuation funds.

AUSTRAC is responsible for administering Australia’s anti-money laundering and counter-terrorism financing regime under the AML/CTF Act and the AML/CTF Rules. AUSTRAC may pursue a wide range of enforcement sanctions under the AML/CTF Act which include

imposing civil and criminal penalties (which can be significant in value), enforceable undertakings, infringement notices, remedial directions, and power to cancel or suspend registrations of providers of digital currency exchange and designated remittance services. AUSTRAC plays an active role in setting and implementing international standards and is a member of regional and global groups such as the Financial Action Task Force and the Asia/Pacific Group on Money Laundering.

The Office of the Australian Information Commissioner (**OAIC**) administers the *Privacy Act 1988* (Cth) (**Privacy Act**) which regulates the handling of personal information by Federal government agencies and some private sector organisations. The Privacy Act includes 13 Australian Privacy Principles (**APPs**), which impose obligations on the collection, use, disclosure, retention and destruction of personal information. The APPs extend to an act done, or practice engaged in, outside Australia by an organisation that has an “Australian link” (including where it carries on business in Australia and has collected or held personal information in Australia, either before or at the time of the act or practice).

Fintechs may also be subject to the prohibitions laid out in the *Australian Consumer Law*, which is enforced by the Australian Competition and Consumer Commission (**ACCC**). Broadly, these include prohibitions on misleading and deceptive conduct, false or misleading representations, unconscionable conduct and unfair contract terms. Whilst the *Australian Consumer Law* does not apply to financial products or services, many of these protections are enforced by ASIC either through mirrored provisions in the *Australian Securities and Investments Commission Act 2001* (Cth) (**ASIC Act**) or through delegated powers.

The Reserve Bank of Australia is Australia’s central bank and provides a range of banking services to the Australian Government and its agencies, overseas central banks and official institutions. It is also responsible for maintaining the stability of the financial system through monetary policy and regulating payment systems.

The Fair Work Commission is Australia’s national workplace relations tribunal and is responsible for administering the provisions of the *Fair Work Act 2009* (Cth) (**Fair Work Act**), which governs the regulation of employment in Australia. In relation to hiring, minimum terms and conditions of employment for most employees (including professionals) are governed by modern awards, which sit on top of the National Employment Standards. The Fair Work Commission’s powers and functions broadly include dealing with unfair dismissal claims, anti-bullying claims, unlawful termination claims, setting and reviewing minimum wages in modern awards and making orders to stop or suspend industrial action.

Key regulations and regulatory approaches

Regulatory framework for fintech businesses

Fintech businesses must comply with the applicable licensing, registration and disclosure obligations under Australia’s financial services regime.

Fintech businesses carrying on a financial services business in Australia must hold an Australian financial services licence (**AFSL**) or be exempt from the requirement to be licensed. Financial services are broadly defined under the *Corporations Act 2001* (Cth) (**Corporations Act**), which is administered by ASIC, to include the provision of financial product advice, dealing in financial products (as principal or agent), making a market for financial products, operating registered schemes and providing custodial or depository services. A financial product is a facility through which, or through the acquisition of which, a person makes a financial investment, manages a financial risk or makes a non-cash payment.

The Australian credit licence (**ACL**) regime applies to entities who engage in consumer credit activities in Australia, such as providing credit under a credit contract or consumer lease. Fintech businesses that provide marketplace lending products and related services will constitute consumer credit activities and will generally trigger the requirement to hold an ACL, or otherwise be exempt from the requirement to hold an ACL. Consumer credit activity is regulated by ASIC and under the *National Consumer Credit Protection Act 2009* (Cth) and associated regulations.

Fintech businesses may also need to hold an AML where they operate a facility through which offers to buy and sell financial products are regularly made (e.g., an exchange). If an entity operates a clearing and settlement mechanism which enables parties transacting in financial products to meet obligations to each other, the entity must hold a clearing and settlement facility licence or be otherwise exempt.

As discussed above in “Regulatory bodies”, the Privacy Act regulates the handling of personal information by Federal Government agencies and some private sector organisations. In 2018, the Notifiable Data Breaches (**NDB**) scheme was introduced and mandates that entities regulated under the Privacy Act are required to notify any affected individuals and OAIC in the event of a data breach (i.e., unauthorised access to or disclosure of information) which is likely to result in serious harm to those individuals. The NDB scheme applies to agencies and organisations that the Privacy Act requires to take steps to secure certain categories of personal information.

Fintech innovation and regulatory developments

Australian regulators and policy-makers in the financial services sector have sought to improve and engage with technology-focused businesses. The financial services regulatory regime adopts a technology-neutral approach so that services are regulated equally, irrespective of the delivery method. Regulators have supported the market entrance of fintechs by streamlining access and offering informal guidance to enhance regulatory understanding. Both ASIC and AUSTRAC have established Innovation Hubs to assist fintech businesses more broadly in understanding their obligations under Australian law. ASIC’s Innovation Hub provides tailored information and access to informal assistance intended to streamline the AFSL process for fintech start-ups. AUSTRAC’s Fintel Alliance also has an Innovation Hub targeted at combatting money laundering and terrorism financing and improving the fintech sector’s relationship with government and regulators.

In December 2016, ASIC issued instruments establishing a fintech licensing exemption and released regulatory guidance detailing its regulatory sandbox for fintech businesses to test financial services, financial products and credit activities for up to 12 months without holding an AFSL or ACL. There are strict eligibility requirements for both the types of businesses that can enter the regulatory sandbox and the products and services that qualify for the licensing exemption.

Restrictions

At the time of writing, there have not been any prohibitions or restrictions on fintech business types. Australian regulators and policy-makers have generally sought to encourage and support fintech businesses, provided such businesses comply with applicable laws (including financial services and consumer laws). However, as discussed above under “Approaches and developments”, regulators have begun moving from observational positions to enforcement with respect to fintechs. For example, in September 2018, ASIC took action against five ICOs targeting retail investors for failure to comply with the relevant licensing and disclosure laws.

Cross-border business

Cross-border collaboration

Australian regulators and policy-makers have sought to improve their understanding of, and engagement with, fintech businesses by regularly consulting with industry on proposed regulatory changes and entering into international cooperation and information-sharing agreements. ASIC has entered into a number of cooperation agreements and information sharing agreements with overseas regulators for the purpose of facilitating cross-border financial regulation and removing barriers to market entry. Under these arrangements there is a sharing of information on fintech market trends, encouraging referrals of fintech companies and sharing insights from proofs of concept and innovation competitions. Through these agreements, regulators hope to further understand the approach to regulation of fintech businesses in other jurisdictions, in an attempt to better align the treatment of these businesses across jurisdictions. ASIC currently has either information sharing or cooperation agreements with numerous jurisdictions, including the China Securities Regulatory Commission, Hong Kong's Securities and Futures Commission, the Monetary Authority of Singapore, the Swiss Financial Market Supervisory Authority, the United States Commodity Future Trading Commission, the Capital Markets Authority of Kenya, Indonesia's Otoritas Jasa Keuangan and Canada's Ontario Securities Commission.

ASIC has also committed to supporting financial innovation in the interests of consumers by joining the Global Financial Innovation Network (**GFIN**), which was formally launched in January 2019 by a group of financial regulators across 29 member organisations. The GFIN is dedicated to facilitating regulatory collaboration in a cross-border context and provides more efficient means for innovative businesses to interact with regulators.

In 2019, a number of fintech associations formed the Asia-Pacific FinTech Network which is designed to facilitate greater collaboration, cooperation and innovation across the region. The network will focus on sectors including regtech, blockchain, payment systems, artificial intelligence and financial inclusion. The network is predicted to accelerate fintech development and lower financial costs both domestically and internationally. At the time of writing, nine countries have formally signed a Statement of Intent.

Passporting

Carrying on a financial services business in Australia will require a foreign financial service provider (**FFSP**) to hold an AFSL or rely on an exemption. At the time of writing, Australia has cooperation (passporting) arrangements with regulators in foreign jurisdictions, which enable FFSPs regulated in those jurisdictions to provide financial services to wholesale clients in Australia without holding an AFSL. Before providing financial services, they must disclose to clients that they are exempt from holding an AFSL and that they are regulated by the laws of a foreign jurisdiction.

ASIC has announced that it will be proceeding with a proposal to repeal passport relief and will implement a new regime that will require FFSPs to apply for a foreign AFSL (i.e., a modified form of an AFSL for FFSPs). Passport relief will cease to be available from 30 September 2019.

Cross-border business

In June 2018, the Australian government passed the *Corporations Amendment (Asia Region Funds Passport) Act 2018* (Cth), which incorporates the Asia Region Funds Passport (**Passport**) into the Corporations Act. The Passport is a region-wide initiative to facilitate the offer of interests in certain collective investment schemes established in Passport member

economies to investors in other Passport member economies. It aims to provide Australian fund managers with greater access to economies in the Asia-Pacific by reducing existing regulatory hurdles. Australia, Japan, Korea, New Zealand and Thailand are all signatories to the Passport's Memorandum of Cooperation. While the Passport officially launched on 1 February 2019, at the time of writing, Australia is the only participating economy to have passed laws to enable the Passport to operate.

In addition to the Passport, the Corporate Collective Investment Vehicle scheme (**CCIV**) will be a new type of investment vehicle that aims to expand the range of collective investment schemes offered in Australia and will enhance the competitiveness of funds by improving access to overseas markets. The CCIV regime is intended to complement the Passport, which will allow Australian fund managers to pursue overseas investment opportunities through a company structure. Public consultation on the third tranche of legislation closed on 26 October 2018 and two draft Bills implementing the CCIV regime were released for public consultation on 17 January 2019.

**Peter Reeves****Tel: +61 2 9263 4000 / Email: preeves@gtlaw.com.au**

Peter Reeves is a partner in Gilbert + Tobin's Corporate Advisory group and is an expert and market-leading practitioner in financial services regulation and funds management. He leads the Financial Services and Fintech practices at G+T. Peter advises domestic and off-shore corporates, financial institutions, funds, managers and other market participants in relation to establishing, structuring and operating financial services sector businesses in Australia. He also advises across a range of issues relevant to the fintech and digital sectors, including platform structuring and establishment, payment solutions, blockchain solutions and global crypto-asset strategies. *Chambers 2019* ranks Peter in Band 1 for Fintech.

Gilbert + Tobin

Level 35, Tower Two, International Towers Sydney, 200 Barangaroo Avenue, Barangaroo, Sydney NSW 2000, Australia
Tel: +61 2 9263 4000 / Fax: +61 2 9263 4111 / URL: www.gtlaw.com.au

Brazil

Vinicius Sahione, Alexandre Vargas & Luiz Felipe Di Sessa
Cescon, Barriau, Flesch & Barreto Advogados

Approaches and developments

In recent years, several new rules and guidelines have been proposed and/or introduced by the financial and capital markets authorities in Brazil to foster the innovation and creation of new players within payment, peer to peer lending, personal finance management and blockchain/distributed ledger technology segments. Currently amounting to over 400 “fintechs” nationwide (according to a survey carried out in 2018 by *FintechLab*),¹ the fintech industry received over BRL 1.5 billion in investments in 2018. Since 2013, the year in which the legislation for payment arrangements was enacted, a growth in fintechs has been observed in Brazil.

The Brazilian Central Bank (“**Central Bank**”) has attempted to reduce the influence of several players in the payment services chain (e.g. by restricting exclusivity contracts with credit card networks) in the past few years, thus encouraging the growth of smaller acquirers and fintech startups and stimulating the competition in this segment. The Central Bank also enacted in 2018 a regulation for peer-to-peer lending (“**P2P**”) companies and direct credit companies, with the purposes of providing legal certainty to the segment of electronic credit platforms and reducing the influence of fully-fledged Financial Institutions over fintech and innovation (see “Key regulations and regulatory approaches” section).

Cryptocurrencies and distributed ledger technology have also recently been at the centre of debates, although decisive guidance on the matter is yet to be provided by the Central Bank and the Brazilian Securities and Exchange Commission (*Comissão de Valores Mobiliários* – “**CVM**”) (see “Key regulations and regulatory approaches” section).

Fast payments – impending changes to payments processing

All financial transactions in Brazil are carried out within a “real-time gross settlement system” created by the Central Bank – the Reserve Transfers System (*Sistema de Transferência de Reservas* – “**STR**”). This system is maintained and operated by the Central Bank and is based on the real-time transfer of funds between its participants.

A relevant impending change related to the STR is the implementation of a “fast payment system” in Brazil, currently adopted by several countries.² In 2018, the Central Bank created a working group for “fast payments” (“*pagamentos instantâneos*”) to design a substitute for the current system authorised to settle payment transactions (i.e. CIP, described in the “Key regulations and regulatory approaches” section). The Central Bank working group’s final report indicates that an independent “real-time gross settlement system” will be created exclusively to process “fast payments”, continuously operational (i.e. 24/7), to be fully operated by the Central Bank.³ Such system is expected to be ready for testing in 2020 and fully operational by 2021.

Fintech offering in Brazil

The fintech offering in Brazil ranges across several financial services. According to numbers given by “*Radar FintechLab*” in August 2018, among the 404 fintechs considered in their research, the payments sector has the largest percentage in the total number of companies (26%), followed by Credit Fintechs (17%), financial management (17%) and insurance (9%), i.e. InsurTech (as defined in the sub-section “Regulatory and insurance technology” below). Other areas include cryptocurrencies and distributed ledger technology (7%), investments (6%) and digital banking (2%).

The largest recent investments in fintechs in Brazil have also been allocated to the payments and credit fintech industries, including the two Initial Public Offerings (“**IPOs**”) of Stone and PagSeguro (both fintechs focused in acquiring business, independent from fully-fledged Financial Institutions, which also offer pre-paid accounts/e-wallets).

In its turn, the “*Fintech Deepdive*” research conducted by the Brazilian Fintech Association (*Associação Brasileira de Fintechs* – “**ABFintechs**”) and PricewaterhouseCoopers (PwC) indicates that 67% of fintechs expect to grow by more than 30% in 2018, *vis-à-vis* an expectation of 50% in 2017.

Considering the most recent regulatory framework (as described below) and regulatory approach adopted by the Central Bank, the fintech industry is expected to continue growing in the following years.

Regulatory and insurance technology

Regulatory technology (“**RegTech**”)

In recent years, the rapid pace of digitalisation and the increasing use of mobile/internet to access financial and payment services has presented intense challenges to Financial Institutions and other institutions subject to the Central Bank’s supervision (such as payment institutions, as defined in the “Key regulations and regulatory approaches” section). In particular, these challenges pertain to compliance with applicable anti-money laundering (“**AML**”) and know-your-client (“**KYC**”) regulations. In this context, technology has been intensely applied by startups and technology companies to ease/streamline the procedures for compliance with such regulations (RegTech).

Several initiatives have been born in Brazil to that effect. Startups specialised in AML/KYC have applied artificial intelligence, machine learning, optical character recognition, and voice recognition, among other technologies, in order to aid companies to comply with AML/KYC regulations imposed by the Central Bank, the CVM and the Financial Activities Control Council (*Conselho de Controle de Atividades Financeiras* – “**COAF**”). The latter is responsible for collecting and processing information regarding potential money-laundering activities that have been reported by market players (such as Financial Institutions and payment institutions) to the competent authorities.

In its turn, the Central Bank created “*Lift Lab*”, an innovation lab in technical cooperation with relevant technological infrastructure players (such as Amazon, Microsoft, Oracle, IBM, among others), under the concept of a “sectorial sandbox”.⁴

Among projects developed within the “*Lift Lab*” in 2018 were RegTech projects aimed at providing the Central Bank and market players alike with better quality, reliable information. For instance, one project applies artificial intelligence techniques, including “deep learning”, to aid in the decision-making process for the extension of loans. The software suggests credit limits, number of instalments for payment, interest rates, and the percentage of the

income that may be committed by the borrower, among other aspects. This is positive for Financial Institutions, since its AML/KYC policies may be streamlined to detect anomalies in credit card spending with the aid of machine learning.

Another project applies machine learning techniques to provide intelligence stemming from contacts between Financial Institutions and their clients by way of call centres/telephone contacts. By “learning” what is the usual/standard pattern of credit card expenses of any given customer/group of customers, the software is able to detect uncommon patterns, which may constitute fraudulent activity.

Considering the examples above, machine learning and artificial intelligence may aid Financial Institutions not only in reducing the percentage of fraud (lowering the overall cost of credit), but also regarding loans/offering of credit to obtain greater efficiency regarding the capital immobilised to comply with minimum capital adequacy ratios (Basel Committee). For that end, the Financial Institutions credit policies may be streamlined to the actual credit risk carried by each borrower.

Insurance technology (“InsurTech”)

From established companies to startups, Brazilian insurance companies are increasingly applying fintech to their services or products (InsurTech). The application of fintech, subject to compliance with data protection laws, may allow insurance companies to improve their risk management, leading to new products based on particular needs and creating a better consumer experience for their clients.

For instance, there are examples of InsurTechs that employ technology to help autonomous insurance brokers selling vehicle protection insurance policies in their integration with clients, where brokers are registered on an electronic platform (through mobile phone applications). The use of fintech vastly increases the efficiency in the search, pricing the hiring of new insurance policies, thus benefiting all players involved (brokers and clients).

InsurTech in Brazil is currently not covered by any specific regulation.⁵ The current regulatory model adopted by the Superintendence of Private Insurance (*Superintendência de Seguros Privados* – “SUSEP”) is based on two main pillars: systemic health; and social adequateness of the insurance activities. In line with such principles, the regulatory approach adopted by SUSEP is that of exercising strict control over the proposal of new distribution models and to seek the standardisation of insurance contracts.

This is evidently a challenge for the InsurTech industry, which is based primarily on technology and innovation. These entities shall either: **(i)** obtain SUSEP’s prior authorisation to operate; or **(ii)** establish partnerships with fully-fledged insurance companies to offer their services, although InsurTechs providing pure technology services may fall outside the scope of SUSEP regulation. Apart from the authorisation to operate, SUSEP may also require regulated entities to hold specific certification related to their segment of activity in the insurance market.

Regulatory bodies

Although fintech is not regulated as an industry in Brazil, the regulatory burden of the financial and capital markets tends to fall upon rising fintechs. The Brazilian Financial System does not adopt a “twin peaks” regulatory approach, such as the one adopted in the United Kingdom, Australia and other countries. Rather, the highest regulatory authority in the Brazilian Financial System is the Brazilian National Monetary Council (*Conselho Monetário Nacional* – “CMN”), and other authorities regulate specific areas within the Brazilian Financial System.

Financial services fall under the regulatory scope of the Central Bank and the CMN, including banking activities, payment services, lending and credit card network schemes, among others. Activities in the Brazilian capital markets, such as securities intermediation, public offerings of securities, securities research, consulting and portfolio management are regulated by the CVM. Private insurance services are regulated by SUSEP.

Fintechs providing services regulated by such entities may be subject to authorisation to operate. In such case, requesting authorisation or, alternatively, entering into partnerships or joint ventures with regulated entities (such as Financial Institutions or brokers) should be considered, while fintechs that provide pure technology services (or back-office activities) are not commonly regulated. Fintech is part of the Brazilian Central Bank's "*BC+ agenda*", which aims at fostering innovation to increase competitiveness in the credit segment, thus reducing costs for final users and promoting financial inclusion, one of the principal pillars of the Brazilian Central Bank's monetary policy.

Key regulations and regulatory approaches

The fintech ecosystem in Brazil is largely composed by the payments and Credit Fintech industries. Below we provide the most relevant regulations and regulatory approaches to these two sectors ("Payments in Brazil" and "Credit Fintechs in Brazil"), as well as recent development regarding the offering and trading of cryptocurrencies in Brazil ("Cryptocurrencies/Tokens in Brazil") and the use of "robo-advice" in the Brazilian capital markets ("'Robo-advice' in the Brazilian Capital Markets").

Payments in Brazil

The Brazilian Payments System (*Sistema de Pagamentos Brasileiro*) has undergone deep changes since 2013 following the enactment of Law No. 12,865 ("**Payments Act**"). In the view of the Brazilian government and of the market as a whole, the Payments Act is an important step forward in promoting financial inclusion, innovation, competition and the decentralisation of the payments industry in Brazil.

As mentioned below, there are a few examples of sandboxes that have helped foster the fintech scene in Brazil (see sub-sections "Payment Networks" and "Payment Institutions"). Among other reasons, minimum thresholds for relevant Payment Networks and Payment Institutions (as defined below) were created to foster the fintech/innovations scene in Brazil, given that an early authorisation process with the Central Bank and the regulatory burden stemming thereof could inhibit new "fintechs".

Payment Networks

Under the Payments Act, a payment network/payment scheme is the set of rules and procedures governing the provision of a certain payment service or scheme to the public that is accepted by more than one receiving entity ("**Payment Network**"). The Payment Network itself does not perform payment activities, but rather governs the set of rules related to a particular payment service (e.g. credit card, prepaid card or payment accounts P2P transfers). Payment services, on the other hand, are carried out by the Payment Network's participating institutions (mainly by Payment Institutions, as defined below).

In view of their relevance to the Brazilian Financial System and as a general rule, Payment Networks are subject to prior authorisation from the Central Bank. Pursuant to Central Bank data, as of February 2019, 12 Payment Networks were authorised to operate in Brazil and 33 Payment Networks were undergoing the authorisation process.⁶ This evidences the growth potential of the payments industry in Brazil and the market's current concentration in a few players.

Non-regulated Payment Networks and those exempted from Central Bank regulation

As a general rule, Payment Networks are part of the Brazilian Payments System. However, certain Payment Networks are not subject to the Central Bank's oversight. Payment Networks are classified as "non-regulated" based on the nature of the entity (e.g. "private label" payment networks, public services or benefits, such as food stamps and culture vouchers), volume of transactions or relevance to the Brazilian Financial System (to be assessed on a case-by-case basis).

Moreover, Payment Networks under the "regulatory sandbox" concept transact less than **(i)** BRL 500 million in amount of payment transactions, or **(ii)** BRL 25 million in number of payment transactions, on a consolidated basis, in a given 12-month period.

Since 2014, the number of non-regulated Payment Networks in Brazil has increased by over 50% (from 109 to 164 in total numbers).

Payment Network Owner

A Payment Network Owner is the legal entity responsible for the Payment Network ("**Payment Network Owner**"). Under Central Bank's Circular No. 3,682, these entities shall enact rules and procedures to be followed by Payment Network participants, including settlement procedures, risk management and minimum operational standards regulations, as well as the applicable penalties. In Brazil, Payment Network Owners are commonly denominated "*bandeiras*" (e.g. Visa, MasterCard, Elo, etc.).

Payment Network Owners shall have a physical, technical and financial structure that is compatible with the relevance of the payment activity performed by its Payment Network(s) and are subject to stringent reporting and diligence duties.

Payment Institutions

A Payment Institution is the legal entity that enables final users to perform payment transactions or the transfer of funds by joining one or more Payment Networks ("**Payment Institution**").

Under Central Bank's Circular No. 3,885, as a general rule, Payment Institutions must request for the authorisation to operate with the Central Bank and are subject to continuous oversight. According to Central Bank data, as of March 2019, approximately 1,000 non-Financial Institutions were rendering payment services in Brazil. In contrast, to date only 11 Payment Institutions are authorised to operate.⁷

Payment Institutions are classified as: **(i)** issuers of electronic currency, typically the offering of e-wallets/pre-paid account services); **(ii)** issuers of post-paid Payment Instruments (as defined in sub-section "Payment Instruments" below), typically the offering of services related to the issuance of credit cards); and **(iii)** acquirers, which authorise merchants to accept any given Payment Instrument (both online and offline) and participate in the settlement process on behalf of the merchant.

Certain institutions, despite rendering services that are restricted to Payment Institutions, can operate without needing prior authorisation from the Central Bank.

This is the case of those institutions that participate exclusively in "private label" or benefit Payment Networks, as mentioned in the "Payment Arrangements" sub-section above. As with Payment Networks, Payment Institutions also benefit from a "regulatory sandbox" whenever below the following minimum thresholds:⁸ **(i)** BRL 500 million in payment transactions (period of 12 months); or **(ii)** BRL 50 million in monies deposited in a pre-paid payment account (period of 12 months).

Payment Instruments

A Payment Instrument is the device or set of procedures agreed between the final user and the Payment Institution that triggers any given payment transaction (e.g. a card, payment account, mobile payment, etc.) (“**Payment Instrument**”).

According to latest available Central Bank data, in 2017 the Payment Instruments with most transactions were debit cards (28.4%), *boletos bancários* (“payment slips”) (26.6%) and credit cards (23.3%). At the same time, wire transfers were carried out primarily by means of internet banking (63.2%) and mobile (19.8%).

The numbers above show that the mobile payments market in Brazil has a relevant growth potential. As such, it is gradually being absorbed by start-ups as an alternative to traditional payment means.

Clearing and settlement

Pursuant to Central Bank’s Circular No. 3,682, transactions under the Brazilian Payments System must be settled through a neutral clearing and settlement service provider. The institution chosen by Brazilian Payments System participants to centralise and settle payment transactions was the Interbank Payments Chamber (*Câmara Interbancária de Pagamentos* – “**CIP**”), an entity created in 2001 that provides settlement services.

Under a simplified procedure, the CIP books all transactions carried out within any given Payment Network and allocates the amounts between participants by using a clearing and reconciliation system. Based on the information received, the CIP instructs debtors to make the funds available for settlement and then settles such funds to the creditors.

According to the most recent Central Bank data, in December 2018, the CIP settled an average daily volume of approximately 19.9 million payment transactions and turned an also daily financial volume of BRL 29.5 billion.

Sub-acquirers

Sub-acquirers are an example of non-regulated activity within the Brazilian Payments System. These are entities that, in the regulator’s view, offer relatively low systemic risk to the adequate functioning and stability of the Brazilian Financial System.

Pursuant to Circular No. 3,682, the sub-acquirer is a legal entity responsible for enabling merchants to accept a particular Payment Instrument, but not holding the position of creditor towards the issuer of the Payment Instrument (“**sub-acquirer**”). In Brazil this business model is mainly adopted by “marketplaces”, well-known and widespread digital platforms combining the offering of a place for sellers to advertise their products/services in combination with a pass-through payment solution between end customers and sellers. Sub-acquirers intermediate transactions between acquirers and merchants.

According to Central Bank data, as of March 2019 there were approximately 20 sub-acquirers operating in Brazil. Considering their increasing relevance within the Brazilian Financial System, the participation of sub-acquirers in the CIP’s centralised settlement system is: (i) mandatory as receiver of funds stemming from regulated Payment Networks; and (ii) optional as payer of funds to end users (i.e. merchants) if amounts transacted by the sub-acquirer exceed BRL 500 million in any given 12-month period.

The Central Bank is monitoring this trend and may impose more stringent regulations on sub-acquirers in the future.⁹

Credit Fintechs in Brazil

The direct intermediation of funds (or a credit transaction) in Brazil is a regulated activity

restricted to Financial Institutions. Until recently, fintechs willing to provide credit activities could only operate under the umbrella of a regulated financial institution.

In light of the context above, CMN's Resolution No. 4,656 was enacted with the declared purpose of stimulating competition, encouraging the reduction of interest rates in the credit markets¹⁰ and promoting financial inclusion in Brazil, as a joint effort with the Central Bank's initiatives towards the payments industry (see "Payments in Brazil"). The new regulation created new Financial Institutions under a lighter regulatory regime (as described below), covering loans or financing **(i)** using their own capital, and **(ii)** in P2P lending transactions, as well as related services and activities.

The Direct Credit Company

The Direct Credit Company (*Sociedade de Crédito Direto* – "**SCD**") is a financial institution authorised to grant loans and financing and to acquire credit rights using its own capital, exclusively in an electronic platform environment. The SCD is funded by its shareholders, including investment funds.

Resolution No. 4,656 prohibits the SCD from **(i)** raising funds from the public, except from public equity offerings, and **(ii)** holding equity interest in other Financial Institutions.

The SCD may: **(i)** lend using its own capital; **(ii)** purchase credit rights from third parties; and **(iii)** assign credit rights to other Financial Institutions, securitisation companies or credit rights funds (*Fundo de Investimento em Direitos Creditórios* – "**FIDC**") (which in turn may only offer such credits to qualified investors).¹¹

The P2P Lending Company (Sociedade de Empréstimo entre Pessoas)

P2P Lending Company (*Sociedades de Empréstimo entre Pessoas* – "**SEP**") is a Financial Institution exclusively authorised to act as an intermediary (i.e. a "pass-through" provider of funds) for P2P loans or financing between lenders and borrowers exclusively in an electronic platform environment.

Some restrictions apply to the SEP's activities. It may not assume any credit risk or provide guarantee in the P2P loans intermediated by it and, unless they meet the "qualified investor" criteria (see "Payments in Brazil"), the creditor may not lend more than BRL 15,000 per borrower within the same SEP.

Central Bank oversight

Credit Fintechs shall obtain the Central Bank's prior authorisation to operate as Financial Institutions. They shall be constituted as corporations ("*sociedade anônima*") and maintain a minimum capital and net equity of BRL 1 million at all times. The minimum capital and net equity requirement may be increased depending on a case-by-case analysis to be made by the Central Bank upon receiving the authorisation request.

The Central Bank understands that Credit Fintechs offer limited risk to the stability and orderly functioning of the Brazilian Financial System, considering the limited amounts that are allowed to be transacted by such institutions (*vis-à-vis* fully-fledged Financial Institutions/banks) and their simplified risk profile. As such, Credit Fintechs generally benefit from proportional prudential requirements, which become more stringent as such entities grow.¹²

Finally, the Central Bank authorises Credit Fintechs to render the following services in connection with direct credit and P2P lending transactions: **(i)** credit analysis for third parties; **(ii)** collection services for third parties; **(iii)** insurance representative in the context of direct credit transactions carried out by the Credit Fintechs; and **(iv)** issuer of electronic currency (i.e. e-wallet/pre-paid account provider, as defined in "Payments in Brazil").

Cryptocurrencies/tokens in Brazil

There is no specific law regulating cryptocurrencies/tokens in Brazil. Nonetheless, both the Central Bank and the CVM have issued formal releases expressing their concerns related to this matter with guidelines as to their understanding, as briefly explained below.

Central Bank

The Central Bank does not regulate or supervise transactions performed with cryptocurrencies and, for the time being, understands that such virtual currencies do not bring relevant risks to the National Financial System, especially considering that the cryptocurrency market amounted to only 0.5% of the stock market's total trading volume (according to 2018 numbers).

However, given that the matter has seen growing interest from economic agents, such authority published a formal notice on November 2017 (Notice No. 31.379/17), stating that cryptocurrencies are not issued by any monetary authority and, accordingly, **(i)** do not have any guarantee of conversion to sovereign currencies, **(ii)** are not backed or secured by any real asset of any kind, and **(iii)** their value depends exclusively on the trust conferred by the individuals to its issuer.

Trading platforms are currently not regulated, authorised or under the supervision of the Central Bank (or the CVM). However, the Central Bank has warned the market that if trading platforms come to perform activities restricted to regulated entities (such as brokers), measures may be implemented to restrict such activity.

CVM

Law No. 6,385 defines an asset as a security under the “*collective investment contract*” category if publicly offered to Brazilian residents (please refer to item “2” below), whenever **(i)** investors are granted participation, partnership (or equity) or remuneration rights, and **(ii)** profits arising thereof stem from the efforts employed by the entrepreneur or third parties.

The characterisation of tokens issued and traded by way of distributed ledger technology/blockchain as “*investment contracts*” is currently being treated with caution by the CVM and ruled upon on a case-by-case basis. As in many other jurisdictions, there is some uncertainty with respect to what should trigger the regulatory burden. In a recent precedent (“*Niobium Coin*”), the CVM acknowledged the distinction between: **(i)** “utility tokens” (e.g. Bitcoin and Ethereum), which if publicly offered generally fall within the definition of “investment contracts” under the Brazilian Securities Act and are deemed securities; and **(ii)** “security tokens”, which serve as a “medium of exchange” and should not be treated as an “investment contract”, even if there is an expectation of profits in relation to that token.

Under the Brazilian securities regulations, all public offerings for the distribution of securities must be registered with the CVM and may only be carried out by a registered entity that is a member of the Brazilian securities distribution system. This rule applies to the public offering of “security tokens” (as defined above).

“Robo-advice” in the Brazilian capital markets

The use of “robo-advice” technology in the Brazilian capital markets has been increasing over the past few years.

Aware of this fact, the CVM addressed the matter in CVM Instruction No. 592/17, published in November 2017, through which it set forth general rules and duties for companies providing services of “*guiding, recommending and advising, in a professional, independent*”

and individual manner; on investments in the securities market, whose adoption and implementation are exclusively at the client's criteria" ("Securities Investment Advisory Services").

Among such rules, the CVM expressly clarified that the use of automated systems or algorithms in connection with the rendering of Securities Investment Advisory Services **(i)** is subject to the same rules applicable to the services provided by humans, and **(ii)** does not reduce the consultant liability inherent to the guidance, recommendation and advice provided to clients. Moreover, CVM Instruction No. 592/17 sets forth that companies providing Securities Investment Advisory Services shall keep the source code of the automated system available for the CVM's inspection.

Restrictions

Electronic credit platforms

As mentioned, the direct intermediation of funds (or a credit transaction) in Brazil is a regulated activity restricted to Financial Institutions. One of the main legal structures adopted in Brazil to overcome this restriction prior to the enactment of the regulation of the Credit Fintechs in Brazil (see section "Key regulations and regulatory approaches") was for electronic platforms to operate as banking correspondents (*correspondentes bancários*), which are entities hired by Financial Institutions to render certain financial services to customers on behalf of Financial Institutions (and, thus, acting as a *longa manus* of the financial institution).

This prompted the Brazilian government to act in order to provide legal certainty to the market, as well as to allow electronic credit platforms to operate independently from fully-fledged Financial Institutions. It is yet unclear whether electronic credit platforms still operating as banking correspondents will be required by the Central Bank to request for the authorisation to operate as a Credit Fintech as a condition to resume business. Considering the recent enactment of Credit Fintech regulations and the fact that the market is still adapting to such rules, no restrictive measure in that respect has been taken by the Central Bank to date.

Early payments of merchant receivables

Law No. 12,865 prohibits payment institutions from performing activities that are restricted to Financial Institutions, which are regulated by Law No. 4,595. There is some debate under Brazilian law on whether early payments made by merchant acquirers would constitute a "lending" activity restricted to Financial Institutions. Similarly, there is some debate as to whether the discount rates applicable to this early payment feature should be considered as "interest" under Brazilian law, in which case the limits set by Decree No. 22,623 (the Brazilian Usury Law) would apply to these rates.

Merchant acquirers have since altered their market practice in order to adjust their business model to the Central Bank's current understanding. Since then, early payments to merchants have been provided either by way of **(i)** establishing partnerships with Financial Institutions (not subject to Brazilian Usury Law) so that these can perform early payment activities on behalf of merchant acquirers; or **(ii)** constituting a credit rights funds (*Fundo de Investimento em Direitos Creditórios* – "**FIDC**") which is an authorised vehicle for the acquisition of credit rights under the regulations issued by the CVM.

There is no express regulatory restriction on the purchase price that may be paid by such funds to acquire credit rights.

Cross-border business

Cross-border Payment Networks

The Central Bank's regulations on Payment Networks (see section "Key regulations and regulatory approaches") provide for their classification according to the "territorial scope", i.e. domestic or cross-border. Cross-border payment networks are those in which the Payment Instrument disciplined by the Payment Network (i) is locally issued to be used in other countries, or (ii) is issued abroad to be used locally.

Although not introduced specifically for the fintech industry, being mainly used for the purpose of cross-border card schemes, the cross-border Payment Networks can be an especially useful tool for foreign-based fintechs. In particular, fintechs offering e-wallets to Brazilian residents may connect the local wallets to their international scheme, thus providing Brazilian residents with the opportunity to use monies topped up on the e-wallet for international payments abroad.

Cross-border Payment Networks also benefit from simplified foreign exchange ("FX") procedures whenever the outbound or inbound FX transaction amounts to less than USD 10,000. For transactions below that amount, the FX institution engaged to close the FX rate is not required to execute FX contracts. In order to make the process more straightforward and streamlined, Payment Institutions owning cross-border Payment Networks usually cap the amount that can be transferred to USD 10,000.

Credit Fintechs: authorisation for foreign investment

In October 2018, the Brazilian government edited the Presidential Decree No. 9,544 authorising foreign entities to hold an equity interest of up to 100% in Credit Fintechs (as defined in the "Key regulations and regulatory approaches" section above).

Purpose of the Presidential Decree

Under the Brazilian Constitution, as a general rule, foreign entities are not allowed to hold an equity interest in Financial Institutions incorporated in Brazil. A Presidential Decree is required to establish that the foreign participation is "*of the Brazilian government's interest*".

While fully-fledged Financial Institutions usually obtain a Presidential Decree on a case-by-case basis, the Brazilian government has decided to grant a generic authorisation to foreign participation in Credit Fintechs by means of Presidential Decree No. 9,544. It is especially relevant that the Central Bank has authorised foreign-based investment funds to hold equity interest in Credit Fintechs (however, not exclusively (100%), since one of the shareholders of the Credit Fintech shall be either an individual or a legal entity, not necessarily with residence/place of business in Brazil).

Strategic role of the Credit Fintechs

The regulation of the Credit Fintechs (see the "Key regulations and regulatory approaches" section above) is part of the Central Bank's "*BC+ Agenda*", which aims at achieving a more efficient Brazilian financial system by fostering innovation and following the best international practices.

The generic authorisation granted to foreign participation in the capital of Credit Fintechs aims at attracting global players to foster the development of "*alternative credit*" in Brazil.

* * *

Endnotes

1. *FintechLab* is a hub for connecting and fostering the fintech ecosystem in Brazil, recognised as one of the most reliable sources in the country for data and statistics on fintech. It is responsible for editing the “*Radar FintechLab*”, a biannual report of ongoing fintech initiatives in Brazil.
2. This international trend follows the publication, in November 2016, of “*Fast payments – Enhancing the speed and availability of retail payments*” by the Bank of International Settlements (BIS)’s Committee on Payments and Market Infrastructures (CPMI).
3. A Brazilian fintech named “Swipe Tech” was selected by the Central Bank to develop the infrastructure of the Fast Payments RTGS. Informal estimates indicate that the Fast Payments RTGS will be based on distributed ledger technology/blockchain.
4. The concept of the “*Lift Lab*” is to create a “sectorial sandbox” providing an environment for “fintechs”, established market companies and the regulator to cooperate in the development of new financial products from their conception up to the execution phase within a virtual, controlled environment (i.e. outside the financial or payments markets). The Central Bank highlights that this model benefits from enabling testing without any prudential or systemic risk, in such a way that it does not require any streamlined/customised regulatory structure in order to assess the commercial and technical feasibility of the projects.
5. Nonetheless, in July 2017, the Superintendence of Private Insurance (authority responsible for the supervision and control of the insurance, open private pension funds and capitalisation markets in Brazil) created a Special Commission of Innovation and Insurtech, with the purpose of studying the impacts of fintech in insurance companies and, if necessary, suggesting how to regulate it.
6. Due to discussions between the Central Bank and market participants, the first authorisations to operate for Payment Arrangements (12 in total) were granted in 2018.
7. As discussed below, some Payment Institutions are exempt from the Central Bank’s registration.
8. Payment Institutions can render more than one type of payment service simultaneously. In each case, the minimum thresholds for any of the payment services rendered by the Payment Institution are measured on an individual basis (e.g. an Institution offering pre-paid accounts and acting as a credit card issuer shall measure the thresholds for each payment service separately). As such, a Payment Institution shall request authorisation to operate with the Central Bank for each payment service rendered by it that exceeds the minimum thresholds.
9. The Central Bank has recently publicly consulted market participants, through a public hearing, on the need to convert *sub-acquirers* into *acquirers* when the total amount of their transactions in all of the payment schemes that they participate in is greater than BRL 500 million in the last 12 months.
10. The average interest rates *per annum* in Brazil for the most popular credit lines are among the highest in the world: 119.0% for individuals; and 51.8% for legal entities, as of January 2019.
11. Pursuant to regulations issued by the CVM, qualified investors are any individuals or legal entities with financial investments in amounts exceeding BRL 1 million, as well as investment funds and Financial Institutions, among others.

12. Credit Fintechs are generally part of the “S5” prudential segment (“**S5**”), which provides for prudential requirements tailored to such entities’ reduced size and risk profile. Under the S5, Credit Fintechs and other eligible institutions are required to maintain at all times a minimum Basel Accord capital adequacy ratio (*patrimônio de referência*) of 17% calculated over a simplified risk weighted assets (“**RWA**”) concept. The Central Bank estimates that the amount of capital required of S5 institutions is proportionally smaller than that required of traditional Financial Institutions/banks. Equally important is the less complex calculation method for such capital requirements, which is compatible with the Credit Fintechs’ simplified operational structure. The RWA under the S5 is the sum of the entity’s financial exposure to credit and operational risk.

**Vinicius Sahione**

Tel: +55 21 2196 9239 / Email: Vinicius.Sahione@cesconbarrieu.com.br

Vinicius Sahione has a Bachelor's of Laws (LL.B.) from the Law School of Pontificia Universidade Católica do Rio de Janeiro (PUC-RJ).

Vinicius has significant experience in advising domestic and foreign clients in **(i)** negotiating commercial agreements involving banking and capital markets matters, **(ii)** adapting and structuring foreign-based business models in light of Brazilian banking and capital markets laws, and **(iii)** payment arrangements schemes and solutions under the Brazilian banking law.

**Alexandre Vargas**

Tel: +55 21 2196 9235 / Email: Alexandre.Vargas@cesconbarrieu.com.br

Alexandre Vargas has a Bachelor's of Laws (LL.B.) from the Law School of Pontificia Universidade Católica do Rio de Janeiro (PUC-RJ).

Alexandre has significant experience in advising domestic and foreign clients in **(i)** negotiating commercial agreements involving banking and capital markets matters, **(ii)** adapting and structuring foreign-based business models in light of Brazilian banking and capital markets laws, and **(iii)** payment arrangements schemes and solutions under the Brazilian banking law.

**Luiz Felipe Di Sessa**

Tel: +55 11 3089 6116 / Email: Luiz.Sessa@cesconbarrieu.com.br

Luiz Felipe Di Sessa has a Bachelor's of Laws (LL.B.) from the Law School of Pontificia Universidade Católica de São Paulo (PUC-SP), specialisation in Intellectual Property from the Escola Superior de Advocacia (ESA-SP), and a Master's degree (LL.M.) in Intellectual Property from the World Intellectual Property Organization.

A member of the Technology practice of Cescon Barrieu, he has significant experience in advising domestic and foreign clients in **(i)** negotiating commercial agreements involving IP, IT, data protection and technology-related matters, **(ii)** advising clients in connection with the Brazilian data protection laws, and **(iii)** understanding and overcoming legal barriers applicable to disruptive business and solutions.

Cescon, Barrieu, Flesch & Barreto Advogados

Rua Funchal, 418, 11º andar, CEP 04551-060, São Paulo, Brazil
Tel: +55 11 3809 6500 / URL: www.cesconbarrieu.com.br

Cyprus

Christiana Aristidou & Evdokia Marcou
Democritos Aristidou LLC

Approaches and developments

General developments

Fintech has rapidly developed across the financial industry. The unprecedented high pace of technological evolution, combined with the ever-decreasing barriers to market entry, higher customer expectations, and increasing venture capital, challenge businesses; yet, at the same time, they offer important opportunities for fintech to thrive.

Cyprus is a prime, internationally recognised and reputable financial and business centre by virtue of its business-friendly legal and tax framework, the high quality of services' provision, and the comparative advantages it, generally, presents. This renders Cyprus an attractive place for business. As a jurisdiction that hosts a robust financial industry, which invites and accommodates significant financial actors, Cyprus is receptive to innovative models of financial services and activities.

Cyprus has witnessed considerable growth in fintech during the past five years. This is evidenced by new fintech services offered by:

- start-ups and SMEs (most often in the form of spin-offs); and
- larger, well-established financial services entities which focus on innovation.

Fintech has been warmly embraced by the government, regulators, and financial services actors. Cyprus launched a Digital Strategy in 2012 along the lines of the European Digital Agenda, whereby digitisation and technology constitute the main pillars of the government's strategic plan in modernising the provision of services to citizens. An e-government plan seeks to enhance the use of technology by the government. Information and communication technology are highly promoted in all sectors of the economy, including the financial sector. Further, Cyprus adopted a comprehensive national cybersecurity framework in 2012. Importantly, the Cypriot Government is in the process of preparing a detailed blockchain strategy and report, which is said to be setting out Cyprus' vision for Distributed Ledger Technologies (DLT) and will form part of the wider government's strategy for digital transformation, with the ultimate objective of moving Cyprus to the world of Artificial Intelligence (AI). Furthermore, the strategy is expected to assess and address the risks associated with or arising from the utilisation of these new technologies and the adoption of new models of business and the emergence of new products, which are based on DLT. Within this context, the strategy is expected to look into various different applications of DLT in a variety of sectors and industries.

From a business perspective, fintech companies in Cyprus are currently offering products and services through innovative platform-based models, which fall outside their core

business model. Existing institutions seek to maintain or solidify their position as leading market forces by engaging with fintech start-ups through various forms of collaborative endeavours. Fintech invites smaller businesses to innovate, while forcing incumbents to rely on their market power and benefit from new technologies.

TransferWise naming Cyprus as one of the eight most promising and emerging global technology hubs is only testament to the development of Cyprus in technologies, and especially in the fintech area.

Specific developments

DLT

The domestic financial industry has demonstrated interest in the potential of DLT and, particularly, blockchain at a very early stage of their global emergence. This was probably a necessary business response to the 2013 Cypriot banking crisis and the “haircut” on depositors, which found entrepreneurs, incumbent financial actors, technology-oriented start-ups and other organisations in need of enhancing their financial products and obtaining or providing alternative financing options. The maturity and robustness of the domestic financial industry was also pivotal in enabling the development of fintech-driven services.

The government is currently exploring the application and use of smart contracts, which are said to be given priority in the government’s upcoming relevant strategy on blockchain and DLT. The said strategy is expected to specifically refer to smart contracts that run on DLT and blockchain and to further expand on use cases and potential applications. Based on said strategy, the relevant needs identified therein and the associated risks involved, legislators are expected to proceed to a series of legislative initiatives.

Further, Cyprus Standards (CYS), a member of the International Standardisation Organisation (ISO) as the national standardisation body, participates in the ISO/Technical Committee TC/307 for Blockchain and DLT through approved professionals/national delegates. CYS actively contributes to specialised working and study groups in the areas of Foundations, Security Privacy and Identity, Smart Contracts and their Applications, Governance, and Use Cases. The work undertaken within these groups is mainly directed at issuing international standards, technical specifications and reports concerning smart contracts and their uses. The ultimate purpose of the Committee is to issue a comprehensive list of technical and legal rules. CYS organises specialised events updating and informing policy-makers, the domestic competent authorities, leaders of business unions, and key financial and business actors about the potential of blockchain and smart contracts and the relevant work undertaken by ISO.

The Cyprus Securities and Exchange Commission (CySEC) has shown active interest in shared distributed ledgers, especially in terms of their regulatory potential. CySEC is currently exploring the potential utilisation of shared DLT in developing and enhancing over-the-counter markets’ supervision. CySEC participates in the Blockchain Technology for Algorithmic Regulation and Compliance (BARAC) project, run by University College London (UCL) Blockchain Technologies. The project examines the impact of DLT in the provision of services, regarding, among others, the financial industry that is central to CySEC’s competence. Pursuant to this project, participants explore various approaches of appropriate and effective regulation of novel business models; such models are prominent in the fintech area.

The University of Nicosia has undertaken many initiatives towards developing the application of emerging technologies to business industries, the government, and society. It

is the first university to offer an MSc in Digital Currencies. Furthermore, it has launched the Institute for the Future (IFF), an interdisciplinary research centre which aims to lead in the development of technological innovation in Cyprus, the EU, and globally, and to become a model research centre for exponential technologies. IFF engages with:

- DLT (blockchain);
- virtual and augmented reality;
- robotic applications;
- AI and intelligence augmentation; and
- self-driving vehicles.

The Cyprus Blockchain Association (CBA) is a non-profit association formed with the strategic objectives of promoting the use of, and educating on, DLT and blockchain in Cyprus, by conducting public awareness campaigns, relevant seminars and training. CBA is a founding member of the European BlockTech Federation (EBTF) established in Brussels in 2018, and has signed several Memoranda of Understanding (MoU) with other non-profit blockchain associations. CBA has emerged as a significant national stakeholder that seeks to promote technology, especially blockchain and smart contracts, for the development of the local economy and contribute to the development of a relevant regulatory framework. CBA organises and participates in domestic and international conferences, consults private entities and cooperates with relevant governmental authorities.

Cyprus Blockchain Technologies Ltd, a non-profit organisation, was established for research purposes as a collaboration between academic institutions, local regulators, financial institutions, commercial banks and other technology associations and companies. Indicatively, the University of Nicosia, the Cyprus International Institute of Management, and the two largest commercial banks in Cyprus, i.e. the Bank of Cyprus and the Hellenic Bank, form part of this organisation. The main research fields of the organisation include:

- DLT;
- blockchain;
- digital currencies; and
- bitcoin.

The Research Centre on Interactive Media, Smart Systems and Emerging Technologies (RISE) is another collaboration between the three public universities of Cyprus (Cyprus University of Technology, University of Cyprus, Open University of Cyprus), the Municipality of Nicosia, and international partners University College London and the Max Planck Institute for Informatics. RISE aims at combining academic research and industrial development by enhancing the integration of technologies in society and sectors of the economy.

Invest Cyprus, the island's national investment agency, signed an MoU in October 2018 with the Singapore-registered public blockchain service creator VeChain Foundation, and with the USA-registered blockchain project strategy advisory CREAM on the promotion of DLT on the island. VeChain and CREAM will jointly advise "Invest Cyprus" on issues of public policy that affect economic development with the view of ensuring the efficient use of blockchain in investment and financial services transactions.

Innovation Hub

CySEC launched the "Innovation Hub" with a view to advancing dialogue in the areas of fintech and regtech. Since October 2018, CySEC welcomes applicants eager to see the development of the regulatory framework accommodating emerging financial technologies.

The participants are expected to gain first-hand insight into the implications of the regulatory framework currently underpinning fintech services and products. Further, the participants will be able to provide their recommendations, suggestions and concerns directly to CySEC. The development of the regulatory framework is, thus, anticipated to integrate or at least to consider the views of those directly affected by and involved with the provision of fintech services.

The eligibility criteria for the applicants, as issued by CySEC, demonstrate CySEC's attempt to encourage, support and engage with businesses that are truly innovative. CySEC's Chair has stressed that the Hub was established to encourage the immediate communication between the authority and innovative or new businesses. The Hub welcomes the participation of both supervised and non-supervised entities.

Cryptocurrencies

Virtual currencies have been under CySEC's examination and review, which has recognised and repeatedly pointed out how promising these currencies are. CySEC is also interested in crowdfunding and blockchain-based crowdfunding platforms and has already identified it as a possible means for financing start-ups and early-stage companies.

Tokenisation, i.e. coin/token offerings, a form of crowdfunding usually conducted on DLT platforms which include Initial Coin Offerings (ICO), Security Token Offerings (STO), or Initial Exchange Offerings (IEO), whereby finance is raised in exchange for blockchain tokens, have not yet been specifically regulated. More and more start-up and innovation-driven businesses emerge that seek to raise finance through ICOs. Their limited access to other means of financing pushes them to seek alternative and more cost-efficient solutions. CySEC has recognised their potential and is interested in the development of a regulatory framework that would facilitate their expansion.

CySEC has explained that despite the absence of specific regulation concerning cryptocurrencies, such currencies may be regulated under the existing framework to the extent that they fit within the existing provisions of the relevant legal and/or regulatory framework. Issuing and offering tokens may be caught under the existing regulatory framework, depending on the nature and structure of the relevant tokens. Specifically, it seems that where a token functions as a security, in the same way as traditional securities do, then the relevant securities legislation would apply. A company offering security tokens would have to be public and issue a prospectus, pursuant to the Prospectus Law, unless any exceptions apply. Where, however, a token merely constitutes a utility token, that basically grants its holders access to a business's services, then other consumer-related regulations may, probably, apply. In this regard, Cyprus seems to follow many jurisdictions that have yet to produce comprehensive legislation that directly and specifically addresses token offerings.

CySEC has announced one proposed regulatory intervention related to crypto-asset activities. Cyprus is currently assessing and is expected to release the newest, relevant anti-money laundering (AML) law pursuant to the relevant EU directive. Within the context of the Innovation Hub, CySEC has been contacted by entities involved with crypto-asset activities, which do not seem to fall within the existing regulatory framework. Further to their concerns, and questions, it was decided that some crypto-assets issues should be addressed through the new AML legislation.

CySEC is contemplating the implementation of the parts of the 5th AML Directive that relate to crypto-asset activities. Following the FATF recommendations, CySEC is examining the possibility of including additional points in the domestic legislation, which are not required under the EU AML regime. These include:

- exchange between crypto assets,

- transfer of virtual assets, and
- participation in and provision of financial services related to an issuer’s offer and/or sale of a crypto asset.

Electronic payments

Technology has caused significant developments in the area of electronic payments. The Payment Services Directive (PSD) II, in force since 13 January 2018, has accelerated technological development in the payments area, especially as it requires payment service providers to maintain “open banking” channels, which will secure them access to their clients’ bank account details through banking Application Programming Interfaces (APIs). Further, certain payment surcharge fees have been abolished in relation to specified types of cashless and consumer-related payments within the Single European Payments Area. The final version of the Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA) and Common Secure Communications (CSC) was published in June 2018 to clarify additional measures. The above have led incumbents to technologically improve the provision of payment options to clients. At the same time, fintech start-ups materialise their technology-related expertise to provide efficient payment solutions. E-money institutions have obtained licences from the Central Bank of Cyprus and provide cost-efficient payment opportunities. The European Banking Authority (EBA) aims to provide guidance for market members and help with the implementation of RTS on SCA and CSC, which will come into force in September 2019.

The trend of facilitating and providing efficient payment solutions through electronic and digital means is not Cyprus-restricted. Indeed, mobile payment services are globally recognised for their effectiveness and potential to reach and serve new clients and demographics.

Fintech offering in Cyprus

Cyprus is receptive to technology, which has taken various forms, uses and applications in ways that disrupt, alter and cause the current financial industry setting to evolve. Many technological uses are put in place or considered by many actors in various financial industries in Cyprus. These financial actors include:

- prime brokerages;
- major platform providers;
- liquidity management companies;
- specialist professional services firms;
- regulatory technology companies (regtech);
- reporting companies;
- authorised credit institutions;
- investment firms;
- insurers;
- undertakings for collective investment in transferable securities; and
- other payment institutions.

The leading industries disrupted and developed by various technological uses are 1) the banking industry, 2) the foreign exchange industry, and 3) the investment and wealth asset management industry. These industries, among other industries, have deployed different

technologies and combinations of technology solutions such as blockchain and smart contracts, AI and robo-advisors, data gathering and analytics, augmented and virtual reality solutions, e-signatures, APIs and other algorithm-based software and technology solutions.

As explained above, the government is currently exploring **blockchain** and **smart contracts** for their possible benefits and security in financial transactions and operations. Private entities and companies seem to cause the government's and authorities' interest in these technologies, as they seek to implement these technologies in their models. Blockchain and smart contracts are in the process of implementation in many projects that aim at finance raising. Within this context, entities in the private sector engage with token offerings solutions that make use of these technologies. Blockchain is, also, considered for its potential to store huge amounts of data. This is crucial in the financial industry, where compliance with many finance-related laws requires secure saving and transmission of data.

Blockchain solutions are considered by foreign exchange companies that contemplate setting up crypto-exchanges or providing exchange services with cryptocurrencies. Foreign exchange companies implement other technologies in their business model, with a view to remaining leading financial and economy actors in Cyprus, considering that Cyprus is one of the busiest foreign exchange hubs in Europe. **Algorithm-based technology** solutions, providing automated exchange and investment services, are an important technology application. Investment, asset and wealth management companies research the potential of using DLT alongside **AI** and **robo-advisors** as part of their services. These technologies have not yet been wholly incorporated in their services model, but the direction of these firms is to include these technologies to enhance the provision of their services.

Data gathering and analytics emerge as indispensable tools to financial businesses and the provision of their services. Technology, naturally, impacts and shapes the development of this aspect. Again, the vast amount of data gathered necessitates efficient and accurate handling within the confines of the applicable regulatory frameworks. The most prominent solution is through the use of technology. There is huge potential in deducing finance-related conclusions and trends through data analytics. Financial companies in Cyprus appreciate and seek to rely on this potential.

As explained above, PSD II has caused banks to turn to technology in order to meet their obligations. The use and implementation of **APIs**, as a means to maintaining open banking channels, demonstrates the banking sector's shift to technology-based solutions. Beyond that, incumbent banks seek to apply other technology-based initiatives, probably as a response to technology-driven banking institutions that rely on technology to expedite their services' provision while minimising their fees and costs. Revolut, for example, has recently made its market entrance in Cyprus and has gained noteworthy popularity, precisely owing to the fintech nature of its services. For this reason, incumbent banks turn to **Augmented Reality (AR)** and **Virtual Reality (VR)** solutions to effectuate part of their services. One prominent example is the remote onboarding process, which will facilitate the opening of accounts, even in the physical absence of customers.

Electronic signatures and **other electronic services** enable the provision of remote services not only by banking institutions but also by other financial institutions. The regulatory framework already developed in the EU, and implemented in Cyprus, pertaining to some of these technological developments, has enabled the provision of such fintech services. For example, the electronic Identification and Authentication of trust Services Regulation (eIDAS) regulates some aspects of electronic identification, e-signatures, and other electronic services. eIDAS primarily aims to create an EU-wide framework, where citizens of one

Member State may use their electronic identification (eID) to access the public services of another Member State. Once realised, this will surely create a framework enabling remote services based on technology. Despite referring to the public sector, the model of electronic identification has far-reaching potential exceeding the public sector.

Algorithms and other relevant software allow companies to assess important financial and economic details of customers, such as a customer's credit profile. This is made through data analysis retrieved from a potentially wide range of sources. Technology has started impacting the ways in which entities in Cyprus approach data management and analytics.

Regulatory and insurance technology

Regtech has developed in Cyprus in response to the emergence and expansion of heavy, complex, specialised legislation and/or regulations and/or rules. Businesses are obligated to follow and comply with such a wide range of laws that regtech has seemed to become a viable option for ensuring compliance. Businesses are called to consider how technology may facilitate their reporting obligations. Following the financial crisis, the need to find effective reporting solutions has become even more imperative and acute, especially in the financial area, in light of the expansion of extensive and specialised legislation and/or regulation. AI-based technology is regarded as a potentially useful tool to achieve and implement effective and efficient compliance solutions.

CySEC encourages the involvement of participants in the area of regtech. The Innovation Hub, as described above, focuses on regtech in addition to fintech.

MAP Fintech is a firm that specialises in providing regulatory reporting solutions to obligations that arise in connection with complex and lengthy international and/or EU regulations:

- the EU Markets in Financial Instruments Directive (2014/65/EU) (MiFID II);
- the European Market Infrastructure Regulation;
- the EU Regulation on Energy Market Integrity and Transparency (REMIT) (1227/2011);
- the Dodd-Frank Act;
- the Foreign Account Tax Compliance Act;
- the Common Reporting Standard; and
- the EU Securities Financing Transactions Regulation (2015/2365).

The firm collaborates with Oracle's platinum partner Polaris for the use of its regtech reporting product, Workbench.

No considerable developments have been noted in the insurance technology area, even though some developments and attempts of a smaller scale have been witnessed. Certain events have been hosted by large, domestic organisations that seek to see the development of the insurance technology sector.

Regulatory bodies

Cyprus has not produced any specific fintech regulation and/or legislation that would comprehensively or specifically address fintech. In the absence of a fintech-specific regulatory framework, the fintech area in Cyprus is regulated in the same way as the "traditional" area of finance. For this reason, the regulators and authorities empowered with the supervision of "traditional" financial services and products maintain this power over fintech services.

The Central Bank of Cyprus supervises and licenses the establishment and operation of all payment institutions, including all commercial banks incorporated in Cyprus. The Central Bank is expected to launch an Innovation Hub along the lines of CySEC.

The Superintendent of Insurance is the competent authority of the insurance sector in Cyprus. The Finance Minister has recently announced that the authorities supervising the insurance and pensions sector will be merged into a new, independent authority responsible for the supervision of both these sectors. This means that the Superintendent of Insurance and the Commissioner for Occupational Pension Funds, which is the competent authority for the supervision of the pensions sector, will be replaced by the said new, independent authority. The scope of the competence of the new authority will remain intact when it comes to the insurance sector.

CySEC is the financial regulatory body that is empowered with the supervision, monitoring and general control of the Cyprus Stock Exchange and the investment services sector. CySEC licenses investment services companies, brokers, collective investment funds, fund management companies and consultants and, subsequently, exercises control over such licensed entities. As part of its powers, CySEC may impose disciplinary penalties in relation to breaches of the relevant stock market legislation and/or regulations.

Cyprus follows a sectoral model of financial supervision, meaning that each sector of the financial industry is supervised by a distinct and separate regulator. This means that supervision depends on and is defined by the nature of the financial services and/or activity in question, and the financial sector to which they pertain. Activities that fall under the main financial sectors, i.e. banking, securities and insurance, are subject to distinct authorities' supervision as explained above, contrary to the general tendency in EU jurisdictions where a cross-sectoral model of financial services' supervision is followed. Considering, again, that the supervision and regulation of fintech services does not fall under a regulatory framework distinct from the existing, "traditional" financial services' supervision, fintech services are subject to a sectoral model of regulation and supervision, as well. There has not been any interest in amending the architecture and mode of the financial model of regulation and supervision in light of the development of the fintech area and in anticipation of the further development in this area.

Key regulations and regulatory approaches

Again, Cyprus lacks any legislation and/or regulations targeted towards or directly and explicitly addressing fintech services and products. As stated above, the existing regulatory and legislative framework, as applicable to financial services, shall apply to fintech as well. By no means does the lack of specific and targeted legislation mean that the fintech area is unrestricted. Indeed, the existing framework is potentially applicable to fintech actors and services to the extent that their operations and characteristics, correspondingly, fit within the scope of the existing framework. The relevant legislation that pertains to financial services may apply to fintech services to the extent that such fintech services do not benefit from any exemptions, as provided in the said legislation. Subject to this proviso, the following pieces of legislation are potentially applicable:

- the Business of Credit Institutions Laws 1997 to 2018;
- various EU regulations (which have direct effect in Cyprus) dealing with banking regulation, including EU Regulation 575/2013 on prudential requirements for credit institutions and investment firms;

- the Law on Electronic Money;
- the Provision and Use of Payments Services and Access to Payment Systems Law 2018;
- the Securities and Exchange Commission Law;
- the Transparency Requirements Law;
- the Investment Services and Activities and Regulated Markets Law;
- the Takeover Bids Law;
- the Public Offer and Prospectus Law;
- the Open-ended Undertakings of Collective Investments in Transferable Securities Law;
- the Alternative Investment Fund Managers Law;
- the Alternative Investment Funds Law; and
- the Securities and Stock Exchange Law.

Further regulatory frameworks of a non-financial nature also have potential application to fintech. These include:

- Protection of personal data: EU General Data Protection Regulation (GDPR) (2016/679) and the implementing domestic law.
- Cybersecurity framework: relevant provisions found in the information and communications technology legislative and regulatory frameworks.
- Anti-money laundering: the Prevention and Suppression of Money Laundering and Terrorist Financing Law. The 5th Anti-Money Laundering Directive (2018/843/EC) was adopted in May 2018, which Member States should implement by 1 January 2020. The scope of the Directive extends to and now covers providers of virtual currencies exchange and custodian wallet providers, which need to be registered and comply with the AML Directive.

In relation to cryptocurrencies, again, the existing financial framework applies, as explained above. CySEC has, however, explicitly introduced certain rules that apply to trading in Contracts-for-Differences (CFDs) and/or other derivatives in cryptocurrencies. CySEC has explicitly confirmed that this kind of trading could qualify as trading in financial instruments for the purposes of the relevant existing financial and investments regulatory framework. Engaging in trading activities of this kind would require obtaining a licence from CySEC. Within this context, CySEC has introduced certain rules that aim at enhancing the protection of investors of such CFDs or other derivatives, who must be specifically notified of the possible volatility of cryptocurrencies which underlie such derivatives. In relation to directly trading in cryptocurrencies, or setting up crypto-exchanges, CySEC has not yet clarified its stance. At least for the time being, CySEC does not grant licences to trade directly in cryptocurrencies or to set up a crypto-exchange.

In relation to the securities sector, it must be noted that CySEC has entered an MoU with the UK's Financial Conduct Authority (FCA) with a view to maintaining effective cooperation, exchange of information, supervision and monitoring of both jurisdictions' securities markets after the UK's exit from the EU. The same MoU was entered between all EU/EEA Securities Regulators and the FCA. This will become effective only in case of a no-deal Brexit. This was expected not only because of Cyprus being an EU Member State but also because of the influential role that the FCA and, generally, the relevant UK legal

framework has in Cyprus. This is, possibly, the case because Cyprus is a common law regime and is generally influenced by the UK.

Many of the legislative and/or regulatory developments that relate to fintech are implemented in Cyprus pursuant to various EU regulations, directives or any other law. CySEC has also addressed some fintech-related issues through issuing consultation documents and providing specific rules, such as the rules produced in relation to trading in CFDs of virtual currencies.

Many jurisdictions seek to develop the fintech regulatory area through the introduction of “sandboxes”. Although not a “sandbox” as such, the Innovation Hub may inform the development of the fintech legal framework, as discussed above.

Restrictions

No blanket fintech restrictions

That Cyprus has yet to produce fintech-specific legislation and/or regulation does not mean that businesses are prohibited from carrying out fintech activities in Cyprus. Indeed, companies may exercise fintech activities provided that there is no prohibition to the contrary in the existing regulatory framework. This, however, does not mean that the carrying out of such activities is completely free and open to each business. As explained above, the same restrictions and conditions imposed in relation to the carrying out of “traditional” financial services apply in the case of fintech activities. Companies carrying out fintech activities must comply with the same applicable registration and/or licensing and/or operational restrictions and/or processes as the “traditional” financial services. This is to the extent that the fintech activities fit within the existing finance-related legal framework. Where certain fintech services or products do not fit within the existing framework, there are no explicit prohibitions related to the carrying out or offering of such services or products.

Business incentives

The lack of regulation does not mean that Cyprus does not constitute a welcoming jurisdiction for the provision of fintech activities. There are no business incentives that specifically target fintech activities. Cyprus does, however, constitute a jurisdiction where fintech activities could be carried out smoothly. In general, Cyprus is conducive to the establishment of businesses of many industries and the provision of services, including, obviously, financial services. Cyprus is a common-law jurisdiction, which is well-known to financial actors globally; Cyprus also has a reputable and strong financial industry. Cyprus is fully aligned and in compliance with the EU financial services framework, as required as an EU Member State, and, further, it offers various business incentives.

The favourable business tax framework, in tandem with Cyprus offering access to an extensive Double-Tax Treaty network, encourages business activity in Cyprus. Also, tax incentives are given to start-up companies that are technology driven and may operate in the financial sector. In particular, natural persons investing in qualifying start-ups enjoy income tax relief of up to 50% on their taxable income, subject to a cap of €150,000 per year. Investors can claim tax relief within five years of their investment.

Cross-border business

Fintech, as demonstrated in the above discussion, has considerably impacted and is expected to further impact Cyprus both locally and on a cross-border basis. Cyprus provides the opportunity of such cross-border activities, considering that it does not impose excessive restrictions on cross-border activities when it comes to financial services, including fintech

activities. Cyprus as an EU Member State offers a comprehensive passporting framework, whereby institutions from the EU can benefit from passporting rights and carry out business activities in Cyprus seamlessly.

Passporting may occur in one of the following ways:

- through the establishment of branches in EEA countries; or
- through the provision of services across the EEA on a cross-border basis.

The following entities may passport a single licence across the EU:

- alternative investment fund managers;
- credit intermediaries;
- credit institutions;
- electronic money institutions;
- insurers and reinsurers;
- insurance intermediaries;
- investment firms;
- payment institutions; and
- Undertakings for Collective Investment in Transferable Securities managers.

Also, Cyprus has abolished all exchange control limitations.

Fintech development has impacted both local financial entities and global companies, but has also encouraged the latter to carry out their activities from Cyprus. EU companies may penetrate the local market and offer financial services. Fintech enables the mobile and digital provision of services, thus enabling significant cost reductions; Revolut is an example of such a company. Further, a number of information and communication technology companies from the United States, Europe, Russia and Australia now run their regional headquarters from Cyprus.

Cyprus has signed and become part of the European Blockchain Partnership (EBP). First, this Partnership aims at developing the necessary blockchain-based infrastructure for the provision of cross-border digital services for the public sector. Second, the Partnership aims at expanding the provision of services from the public to the private sector, as well. Such infrastructure has, thus, the potential to facilitate the provision of cross-border services in the financial sector, on blockchain. The Partnership seeks to engage various local economic and financial actors that will ultimately benefit from a cross-border enabling blockchain infrastructure. To this end, any regulatory obstacles hindering such cross-border blockchain infrastructure will be considered and accordingly addressed by the Partnership.

Cyprus, along with Malta, France, Greece, Italy, Portugal, and Spain signed the joint “Declaration of the Southern Mediterranean Countries on DLT” with a view to enhancing cooperation between these states and furthering the position of Southern Europe as an emerging technologies leader.

The International Standards on blockchain and smart contracts that are to be published by the ISO will go a long way towards facilitating cross-border provision of services, including fintech services. These standards aim at achieving the compatibility and interoperability of these technologies, thus eliminating cross-jurisdictional issues that might arise.

**Christiana Aristidou****Tel: +357 99 45 30 19 / Email: christiana@aristidou.com**

Christiana Aristidou is an International Business and Technology Lawyer with more than 22 years of practice. She is a Certified International Legal Project Practitioner (LPP) and has been a litigator since 1997. Christiana is a National Delegate to the ISO TC/307 for Blockchain and DLT and a founding member and Vice-president of the Cyprus Blockchain Association.

A recognised expert in the fields of technology, business, commercial, international tax, finance, intellectual property, e-commerce, investment and securities laws, Christiana has been involved in, advised and managed complex business and technology legal projects involving major foreign legal jurisdictions and a variety of legal and regulatory frameworks. She possesses exceptional skills in comparative law.

She is currently focused on innovation and the emergence and use of exponential technologies, start-up and spin-off projects, ICOs, STOs and LCOs, and she is researching blockchain, DLTs and smart contracts.

Christiana is a legal author and policy influencer with numerous publications and articles in various journals, legal magazines, databases and on social media.

**Evdokia Marcou****Tel: +357 99 72 51 31 / Email: e.marcou@aristidou.com**

Evdokia has been working as a lawyer for the past year, after having completed her studies in the UK. Her strong academic background and her dynamic training enabled her to immediately take part in complex, multi-sectoral projects. She has been involved with corporate law, banking and finance, and IP-related matters, while focusing, at the same time, on technology-oriented issues. Within this context, she conducts research in blockchain-related law, including blockchain-based uses and applications for the public and private sectors, while participating in ICO and STO projects. She has provided legal opinions and consultation on the areas of banking and finance, IP law, and corporate law. Evdokia is driven, hardworking, and committed to constant self-improvement and learning.

Democritos Aristidou LLC

80, Georgiou G. Digheni Avenue 3101, 3101 Limassol, Cyprus
Tel: +357 25 58 58 11 / URL: www.aristidou.com

Czech Republic

Petr Vybíral & Tomáš Kirner
Allen & Overy (Czech Republic) LLP

Approaches and developments

Revolutionary IT solutions are changing the nature of the financial sector globally by pervading all its crucial segments – in particular banks and credit institutions, insurance, funding, capital and financial markets, capital raising, payments and payment services. The rapid growth of the regulatory burden, which accelerated after the 2008 financial crisis, significantly contributed to the evolution of Fintech. For the purpose of this chapter, we will further refer to Fintech with the meaning of technology developments and innovative solutions that are emerging in the financial services sector in any form. A prerequisite to successful and ongoing Fintech development is, without any doubt, corresponding regulatory response. The establishment of sensible regulation which would promote a favourable level of development and mitigate the corresponding risks to the broadest extent possible at the same time is up to the relevant authorities.

Following the emergence of Fintech companies on the Czech financial market, legal professionals started to discuss the benefits and disadvantages of the implementation of new regulation in the Czech Republic. The development of new rules, however, has not gone beyond discussion among start-ups, incumbents, legislators and the Czech National Bank (CNB), the latter of which has the role of a full-scope regulator of the Czech financial and insurance market. Therefore, we have not, until now, seen a single new law (or other set of rules) reacting directly to Fintech issues, unless previously approved at the European Union (EU) level.

The Ministry of Finance issued two public consultations regarding Fintech topics at the turn of 2018 and 2019. The first one looked more generally at various future trends and necessary changes to the regulation of the Czech capital and financial markets. The second, called “Blockchain, virtual currencies and assets (use of blockchain technology for records of securities)” (**Blockchain Consultation**) was more focused and dealt only with the implementation of distributed ledger technology into the Czech capital and financial market regulatory environment. The potential outcome of the consultations is the introduction of legislative changes to some of the current challenges brought by Fintech. We will discuss some ideas made in these public consultations below, as these provide the best picture as to what the Czech government and its legislation will likely aim for in the near future.

Besides various efforts for legislative changes, the CNB also regularly provides valuable information for participants and other stakeholders in the Czech capital and financial markets by virtue of producing and publishing official guidance (or statements) and addressing various topical legal issues, through providing answers to reasoned (so-called qualified) questions (formal Q&A tool) of such market participants, their advisers and other

stakeholders active in the Czech financial services sector. Recently, the CNB created a special department for payment services and financial innovation which shall assist market participants and the government with preparations for legislative changes. According to public reports, the CNB's approach to Fintech is based on three main principles: “(i) *technological neutrality*, (ii) *consistent application of current regulatory rules* and (iii) *openness to discussing individual innovative cases*.”¹

However, the CNB's official guidance and statements or answers to reasoned questions (i.e., guidance available through the formal Q&A tool) are considered *soft law* only and as such do not necessarily set firm cornerstones for potential future legislation in the Fintech area. Above all, currently, while the Czech business sector is rather vocal and, as a priority, demands unification of the rules across the EU to allow start-ups and other companies or businesses to conduct their activities on a cross-border basis, we do not expect Czech legislation to take any steps that would substantially divert the Czech legal framework from any directions made at the EU level.

The minimalistic approach of Czech regulators and legislators is incomparable with regulatory leaders like China, Japan, the UK or the US, which have introduced changes and provide their market participants with ongoing support in the form of sandboxes and other practical measures, making sufficient room for further efforts in implementing new Fintech technologies. By the same token, the lack of new laws or rules does not prevent local Fintech start-ups from disrupting the incumbent local capital markets and financial and payment services environment with a broad range of unregulated technologies and practices.

A good example of a successful initiative is the project SONIA, introduced by the Czech Banking Association (CBA). The aim of this project is to create a digital personal identity to be used for online communication between individuals and companies or public institutions. The functionality of the system would allow distance identification of individuals via their banking identity; i.e., log-in details they use for internet banking. This is not a major novelty, but is certainly an important and good step forward, whilst similar systems already function in Canada, Denmark, Sweden and the UAE.²

Fintech offering

Payments and payment services

The global banking sector has recently experienced significant transformation. Due to the gradual changes in regulation over the past few years, new players have emerged in the market, and the traditional financial institutions as we know them are facing a huge challenge. In order to retain their market power, as the competition increases, these institutions are pushed towards implementing new technologies, innovative features or setting up joint ventures or cooperative agreements with start-ups to provide final customers with high-end services.

Following the implementation of Payment Services Directive No. 2015/2366 on payment services in the internal market (PSD2) by Payment Systems Act, No. 370/2017 Coll., as amended (PSA), the Czech banking sector has opened ancillary payment services such as multibanking, payment initiation from payment accounts or account balance verification to third party providers (TPPs). Due to delays in the implementation of the regulatory technical standards, the Czech Banking Association has issued the “Czech Standard for Open Banking” to define more specific rules of the functioning of the open banking system among Czech stakeholders. The main reason was to allow banks and TPPs to prepare their application programming interfaces (APIs) and add-on applications to a common standard, and evade increased costs due to versatile implementation of PSA rules. The use of the

standard is voluntary; hence, several banks have already prepared their APIs in line with its recommendations. Nevertheless, the implementation has not been made across the banking sector in completely the same manner and, as such, TPPs may need to amend their applications in line with systems of individual banks.

According to the CBA, the main benefits are the integration of TPPs' applications into banks' systems, uniform interpretation of the PSA, compliance with the content of the transmitted data and security elements in communication with banks, support for the unified functioning of services for clients across banks, and timely readiness for the implementation of the new regulatory rules, provided that the banks maintain a certain degree of freedom in the creation of their own systems.³ To allow communication between a TPP application and a bank's API, the TPP must authorise itself so the bank has ensured that the TPP is indeed the party with whom the bank's system is communicating. For this purpose, the TPP must obtain an electronic certificate containing its private identity. Currently, the Czech payment services market is deciding what certificates will be used. Nevertheless, all of them will most likely have to comply with eIDAS regulation (EU) No 910/2014, which is implemented by the Act on Services Creating Trust for Electronic Transactions, No. 297/2016 Coll.

Virtual currencies and assets

Closely related to payment services are virtual assets recorded on a distributed ledger; i.e., virtual currencies such as Bitcoin or virtual assets (or crypto-assets) produced as utility tokens or security tokens. In January 2019, both the European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA) released reports⁴ on crypto-assets, according to which the majority of crypto-assets, potentially apart from only utility tokens and the like, would qualify as financial instruments (and potentially as transferable securities)⁵ under Directive of the European Parliament and the Council No. 2014/65 on markets in financial instruments (MiFID2).

Based on the ESMA report, the determination of whether MiFID2 applies is crucial, because the applicability of MiFID2 can trigger: prospectus requirements; transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market, if applicable, as implemented in the Czech Republic in the Capital Market Act, No. 256/2004 Coll., as amended (CMA); or rules prohibiting certain trading techniques on regulated markets under Regulation No. 596/2014 on market abuse. The applicability of the conclusions set out in the ESMA report will depend on the structure and governing law of the crypto-assets to be offered and sold in the Czech Republic.

Pursuant to Czech civil law, coins or tokens, as usually issued through initial coin offerings (ICOs) or security token offerings (STOs), running on a distributed ledger, do not fall under the definition of a security and as such are not considered to be investment instruments in the meaning of the CMA.⁶ Consequently, they do not trigger prospectus requirements, transparency requirements or market abuse regulation and generally may be offered and sold to the Czech public without any further consents or licences. Although this interpretation is formalistic, the CNB has already confirmed on several occasions that it is of the same opinion.⁷ Regardless of the above, coins and any kind of tokens may be incorporated into a financial derivative and as such are to be subject to general regulation of investment instruments in accordance with the CMA.

The Czech regulation of investment services relating to virtual currencies or assets is rather less demanding; therefore, an establishment of an ICO or a crypto-currency trading platform does not trigger capital markets regulation. On the contrary, public offer of coins or tokens so issued cannot be easily extended outside the Czech Republic as passporting of their

prospectus under the single EU prospectus regulation framework into another EEA Member State cannot be made. For structuring a public offer, we recommend undertaking specific legal analysis of the applicable Czech and other potentially relevant foreign rules.

The EBA report focuses more on the possibility to classify crypto-assets as electronic money within the meaning of Directive No. 2009/110/EC, on the taking up, pursuit and prudential supervision of the business of electronic money institutions (**EMD2**) or as funds under the PSD2.

The CNB has not indicated its position in relation to those reports as of yet; however, various parties answering to the Blockchain Consultation called for the preparation of brand new bills, or at least some legislative amendments in the area of virtual currencies or assets, in light of and in accordance with the conclusions set out in the EBA and ESMA reports.

According to the CNB's public statement issued in 2014,⁸ Bitcoin or other virtual currencies are not considered scriptural money or electronic money in the meaning of the PSA. Accordingly, they are out of the scope of payment services regulation. Together with the CNB's statements as discussed above, trading with pure virtual currencies (i.e. not forming a part of a financial derivative) is not considered a regulated activity and therefore does not fall under the supervision of the CNB.

Last but not least, pursuant to the Czech AML rules set out in the Act on selected measures against legitimisation of proceeds of crime and financing of terrorism, No. 253/2008 Coll. (**AML Act**), any person who purchases, sells, keeps, manages for a third person or intermediates the purchase or sale of virtual currency, or otherwise provides other services related to the virtual currency,⁹ is an obliged person for AML Act purposes, and as such must comply with the AML rules enacted to help detect and report suspicious activity. This certainly implies that further specific advice should be sought and obtained on various AML-related obligations.

Money exchange

In the case of money exchange offices, we have seen a few attempts to innovate provision of their services on the Czech market lately as well. These businesses each launched an application through which customers (both corporate and private) may exchange their money for dozens of foreign currencies and compare the exchange rate that they offer with the exchange rate of any other bank on the market.¹⁰ No specific money exchange regulation addressing Fintech in this sector has been promoted in the Czech Republic.

Capital raising

Various forms of capital raising have originated on the Czech capital and financial markets, including P2P lending platforms or crowdfunding platforms which offer direct or indirect participations, or plain vanilla notes or structured notes (or investment certificates) issued by start-ups or other marketed companies.

The regulation of each of these platforms heavily depends on the instruments and services it offers. The P2P lending platforms usually possess a light regime licence for the provision of certain payment services under the PSA, or they may also apply for intermediation or provision of consumer loans under the Act on Consumers Loan, No. 257/2016 Coll., where necessary. Crowdfunding platforms may be subject to the CMA or, if they do not offer services connected with investment instruments under the CMA, they may provide their services without an investment firm licence. However, under Section 98 of the Act on Management Companies and Investment Funds, No. 240/2013 Coll. (**MCIFA**), none of these platforms may collect funds from the Czech public for their further reinvestment, provided that profit from the

investment is based on performance of underlying assets into which the collected funds were invested, unless done in line with the MCIFA. This rule effectively prohibits the creation of structures that economically constitute collective investments but are not registered as investment funds and prevent disruptions in the collective investments sector.

Besides the applicable regulation, the platforms must comply with civil law rules, consumer protection rules and marketing rules, and pay taxes in line with applicable legislation.

Client services and internal processes

Besides the product or service innovations described above, it is necessary to also briefly address innovation focused on customer experience when approaching financial services and related internal processes. Customers' needs are coming into the spotlight, which brings opportunity for adaptable Fintech businesses that are able to offer non-traditional and often easier ways to manage their finance and any other related services.

One of the leading Czech banks has recently implemented several bots that help to process internal data in many different areas, especially in processing clients' requests and responding to their questions. Similar systems are also planned to be implemented in the areas of human resources, employment management or advisory services regarding personal investments.

Customers' needs are further targeted by a number of Fintech start-ups that provide online applications, ranging from digital wallets for special purchases or as a replacement for pre-paid card services such as pocket-money apps for children, personal finance apps and cash-back sites to various apps in the crypto universe.

Regulatory and insurance technology

RegTech tools

The emergence of RegTech is attributable to the growth of technological solutions which may also be applied to regulatory processes in order to address challenges that regulators face.

In this sense, the CNB has implemented the so-called "MKT tool" for the purposes of supervision of behaviour of regulated entities active on the Czech capital markets. The MKT tool allows the CNB to process the huge amounts of data received under the local regulation implementing MiFID2, MAR and ancillary regulation governing actions on the Czech capital markets. The purpose of the MKT tool is to monitor potential market abuses and to protect clients active on the Czech capital markets. The participants simply deliver the CNB raw data about their trades and orders, and the CNB then controls the output processed by the MKT tool. As the participants send the data regularly, the delay between the actual trades and supervisory actions is rather short. The MKT tool is also able to include data sources from other EU information exchange mechanisms and to deliver automatic alerts generated on a daily basis.¹¹

In the area of regulation of ICOs, STOs and other Fintech frontiers, the CNB remains rather reluctant and its cautious approach unambiguously prevails. Therefore, the crucial question of whether the ICOs shall be regulated or not remains unsettled, and the CNB has adopted a wait-and-see approach. Nevertheless, to prevent potential market disruptions, the CNB is thought to be using a special tool for initial assessment of ICOs and STOs and their potential impact on the Czech financial market. The tool is called Blackbox (ICO analysis) and shall serve as an initial assessment as to whether an ICO or a STO has a link to the Czech Republic.¹² As this RegTech application is for the CNB's internal purposes only, there is not much information about its functioning available to the relevant stakeholders, let alone the general public.

InsurTech tools

The Czech insurance industry is also reshaping under the emerging technology trends. Some Czech insurance companies have started implementing chatbots together with online sales of insurance products in their portfolios.¹³

Further, a cooperation between insurance companies and start-ups has started functioning in the Czech insurance sector. One interesting project has led to the creation of a new flexible life insurance product that can be purchased or terminated immediately via an online application and offers discounts on insurance premiums for a healthy lifestyle.

Another tool developed by a Czech start-up is a system that can impartially evaluate the pros and cons of each insurance contract (simply by uploading an image of the contract) and utilises a database of various insurance contracts available across the Czech insurance market. Once the contract is uploaded, the tool runs an independent assessment and notifies the client if a more suitable insurance contract was found. The client is then provided with information about the particular insurance company and the alternative insurance conditions.¹⁴

A third interesting InsurTech tool enables entrepreneurs to insure payments from invoices they issue. After submitting the invoice, the insurance start-up takes over control of its administration and undertakes to pay out a certain percentage of the issued amount to the insured entrepreneurs if the customer fails to pay it.¹⁵

All of the aforementioned projects have been made in cooperation with Czech insurance companies, whereas the start-ups participated in the cooperation schemes either as non-regulated entities or as insurance intermediaries that do not have to have such robust internal processes. Accordingly, on the basis of publicly available information, the CNB or the legislator did not have a reason to amend the relevant insurance legislation as the insurance companies are, under the Insurance Act, No. 277/2009 Coll., obliged to comply with outsourcing rules anyway.

The discussion among businesses and the professional public is currently moving towards the deeper implementation of the Internet of Things into the daily business models of insurance companies. It is, therefore, very likely that future innovations in InsurTech will be focused in this way.

Regulatory bodies

Supervision of the financial sector and system

There are two main regulatory authorities in the Czech Republic: the Ministry of Finance, which is responsible mainly for preparation of legislation; and the CNB. The CNB is the central bank of the Czech Republic and the sole national competent and supervisory authority for the capital and financial markets and the entire financial sector and system in the Czech Republic.

Under the Czech Constitution, the CNB exercises its powers directly without any consultations or approvals of other Czech (or European) authorities. In accordance with the Act on the Czech National Bank, No. 6/1993 Coll., as amended (**CNB Act**), the CNB supervises, primarily, the banking sector, capital markets, insurance industry, pension funds, credit unions and payment system institutions.¹⁶ Additionally, the CNB has further powers derived under the Act on Capital Market Supervision, No. 15/1998 Coll., as amended, as well as other special laws and rules regulating the individual sectors of the Czech financial system.

The CNB, acting as the sole national competent and supervisory authority for the Czech financial sector and system, is empowered to supervise activities that are classified as regulated activities according to applicable laws and rules – i.e. activities that are subject to registration or licensing. In other words, if an activity conducted by any Fintech business or entity cannot be classified as a regulated activity, supervision of the CNB cannot be derived from the applicable laws and rules and it is therefore simply out of its scope. The actual use of new technology or implementation of any innovative aspects is then not so relevant.¹⁷

As already mentioned in the opening part of this chapter, in October 2018 a new payment services and financial innovations department was established within the CNB. This department is currently responsible, amongst others, for Fintech regulation on the national level and monitoring of developments in the area of financial market innovation, including virtual or crypto-assets and distributed ledger technology.¹⁸ The current approach of the CNB towards any potential Fintech regulation can perhaps best be described as active monitoring of the market, coupled with cautious but not explicit promotion of any new technologies or innovative developments. In any case, the CNB currently (or for the time being) does not seem to be overly active or otherwise keen to create special rules or a standalone regulatory framework for any Fintech businesses or activities, but at the same time expects that, to the extent that any such businesses or activities would fall within the ambit of the existing laws and rules, they would be complied with.¹⁹

The approach of the CNB is, of course, significantly affected by any relevant approaches taken at the EU level. This would definitely influence the CNB's position towards Fintech. In March 2018, the European Commission released its Fintech Action Plan,²⁰ which aims to encourage implementation of new technologies in the financial sector and increase cybersecurity and integrity of the financial system.

In all these areas, the CNB also cooperates with the EBA, the ESMA, the European Insurance and Occupational Pensions Authority (**EIOPA**), the International Organization of Securities Commissions (**IOSCO**) and others,²¹ whilst the CNB's longstanding best practice has been to implement and follow all opinions, guidance and other soft law documents issued or announced by these agencies in the course of its supervisory and decision-making practice.

Consumer protection

The CNB also supervises consumer protection in relation to entities, which it is obliged to supervise under the CNB Act, or entities licensed under special rules (e.g. investment funds, insurance or reinsurance companies or settlement system operators). The core areas of consumer protection law that are supervised by the CNB are: (i) prohibition of unfair commercial practices; (ii) consumer discrimination; (iii) provision of information about pricing; and (iv) overall compliance with applicable consumer protection regulation.

In respect of certain entities, the consumer protection supervision used to also be performed by the Czech Trade Inspection Authority (in Czech, *Česká obchodní inspekce*) (**CTIA**). The CTIA focused mainly on supervising these businesses and individuals during the negotiation of consumer credit, and their compliance with applicable legal rules. On 1 December 2016, the new act on consumer credit came into effect; namely Act No. 257/2016 Coll. (**Consumer Credit Act**) which set out a one-and-a-half-year transition period, during which responsibility for supervision fully shifted to the CNB. Therefore, the CNB is currently the only supervisory authority in this regard.

Data protection

In the Czech Republic, the area of data protection is supervised by the Office for Personal

Data Protection (in Czech, *Úřad pro ochranu osobních údajů*) (**OPDP**), which is responsible mainly for the supervision of compliance with the broad variety of obligations applicable to the entities that process personal data under the Regulation of the European Parliament and the Council No. 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (**GDPR**), maintenance of the register of notified data processing operations, and dealing with initiatives and complaints from citizens relating to data protection.²² In the case of breach of any obligation under GDPR, the OPDP is empowered to impose administrative fines on violators.

Anti-money laundering

The competent authority supervising the anti-money laundering activities under the AML Act is the Financial Analytical Office (in Czech, *Finanční analytický úřad*) (**FAO**). Besides the monitoring of suspicious market activities, the FAO is also responsible for preparation of various legislative acts, reports and analyses relating to AML/CFT.

Intellectual property rights

Since the Fintech area is also associated with intellectual property rights, the Industrial Property Office (in Czech, *Úřad průmyslového vlastnictví*) is empowered to provide protection in this regard. The protected right will in most cases be the right to protection of software. The Czech law provides many various possibilities for software protection; for example: copyright under Act No. 121/2000 Coll. – on copyright; patentable invention according to Act No. 527/1990 Coll. – the patent act; and its features as a utility model or registered trademark.

Protection of competition

The authority responsible for supervision of competition, public procurement and state aid is the Office for the Protection of Competition (in Czech, *Úřad pro ochranu hospodářské soutěže*) (**OPC**). If any of the predetermined events or thresholds are triggered, the OPC is empowered to act regardless of whether or not a Fintech business is concerned.

Key regulations and regulatory approaches

Since there has been no special regulation adopted so far, generally applicable laws and other rules shall apply in relation to Fintech businesses and activities. The applicable regulations are therefore fragmented and each area or particular aspects are regulated separately. This section aims to provide a general overview of the relevant laws and regulations for each area – both Czech laws and rules and directly applicable EU regulations.

Banking and insurance sector

- Act No. 21/1992 Coll., on Banks, as amended;
- Act No. 87/1995 Coll., on Credit Unions, as amended;
- Act No. 374/2015 Coll., on Recovery and Resolution in the Financial Market, as amended;
- Act No. 257/2016 Coll., on Consumer Credit, as amended;
- Regulation (EU) No. 575/2013, on prudential requirements for credit institutions and investment firms (CRR) including all related delegated regulations;
- Act No. 277/2009 Coll., Insurance Act, as amended;
- Act No. 170/2018 Coll., on Distribution of Insurance and Reinsurance, as amended; and
- various other related or implementing laws, decrees or regulations.

Payments and payment services, electronic money

- Act No. 370/2017, on Payment Systems, as amended;
- Act No. 89/2012, Civil Code, as amended; and
- various other related or implementing laws, decrees or regulations.

Capital markets and securities

- Act No. 256/2004 Coll., on Undertaking Business in the Capital Markets, as amended;
- Act No. 15/1998 Coll., on Capital Market Supervision, as amended;
- Act No. 190/2004 Coll., on Bonds, as amended;
- Regulation (EU) No. 596/2014, on Market Abuse, as amended;
- Regulation (EU) No. 600/2014, on Markets in Financial Instruments, as amended;
- Regulation (EU) No. 1129/2017, on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market; as amended; and
- various other related or implementing laws, decrees or regulations.

Anti-money laundering and combatting the financing of terrorism

- Act No. 253/2008 Coll., on Selected Measures against Legitimation of Proceeds of Crime and Financing in Terrorism, as amended;
- Regulation (EU) No. 2015/847, on information accompanying transfers of funds, as amended;
- Decree of the CNB No. 67/2018 Coll., on Selected Requirements for the System of Internal Rules; and
- various other related or implementing laws, decrees or regulations.

In the Czech Republic, the idea of regulatory sandboxes set by the regulator where Fintech businesses may test their products or services in a controlled environment is currently (or for the time being) only a matter of public debate and discussion among relevant stakeholders. There have been several attempts to bring this up with more parties or the general public – especially various public discussions and conferences organised and realised by the Czech Fintech Association or Institute of State and Law of the Czech Academy of Sciences – but these calls remain, in most cases, unheeded.

The good news is that the CNB holds quite a liberal view on regulatory sandboxes, innovation hubs and other similar initiatives, as long as the principle of equal treatment is sustained and technological neutrality ensured. On the other hand, according to the CNB, since there is no clear distinction between financial institutions in the traditional meaning and Fintech businesses, there is no reason to create a “softer” regulatory environment and more vague conditions for selected market participants. Hence, there are no innovation hubs, Fintech incubators or any other similar concepts that have been implemented by the CNB so far.²³

We are not aware of any shift in attitude in the way the Czech Republic has historically approached Fintech regulation. That is also very likely the reason why there is no big push for changes in the applicable Czech financial sector and system regulation.

Restrictions

The major advantage of the CNB being a bit reserved, or more relaxed, is that no specific restrictions and limitations that would have been imposed over Fintech businesses were created. Therefore, the standard licensing requirements and procedures will have to be applied.

Any Fintech business providing payment services or issuing electronic monies as contemplated by the PSA is obliged to obtain a licence from the CNB. The same applies to potential licensing obligations under the CMA with respect to services and activities that are regulated thereunder, such as provision of investment services dealing in investment instruments or execution of orders in relation to investment instruments. On the other hand, those Fintech activities that do not fall within the applicable rules under incumbent laws and regulations will very likely not trigger any other administrative requirements, such as a necessity to obtain permissions or licences.

Cross-border business

EU regulation generally provides EEA (Fintech) companies with the opportunity to provide regulated services or conduct regulated activities in any other EEA Member State on the basis of a passport. A passport operates as a single licence concept which enables EEA companies to provide their services on the territory of another EEA Member State without the obligation to obtain any licence or permission. The traditional licensing requirement is replaced by notification of the home-state regulator, addressed to the host-state regulator. There are two ways that passporting can happen – the company may establish a branch in the host-state or provide its services on cross-border basis. Entities that may passport their licence include, for instance, credit institutions, payment institutions, investment firms and credit intermediaries. Besides the general laws of the host-state, the home-state prudential rules will apply in respect of passported activities. To the contrary, entities that are not allowed to passport their licence (entities from third countries in particular) need to establish a branch in the Czech Republic and obtain the relevant licence from the CNB in order to conduct the regulated activities on the territory of the Czech Republic.

There is no doubt that Fintech requires proper cross-border regulatory co-operation. Globally, there have been several bilateral memoranda of understanding established and adopted in order to facilitate regulatory cooperation in the area of Fintech. Most of these activities relate to the activities of the International Organization of Securities Commissions (**IOSCO**). Even though the Czech National Bank is an IOSCO member, cooperation in the area of Fintech has not affected the Czech Republic in any regard so far and, formally, there have been no Fintech bridges created between the Czech Republic (or the CNB) and any other country (or its relevant authority) yet.

The CNB closely cooperates with several EU bodies and agencies which subsequently play a significant role in its decision-making. The influence of its approaches is significant, especially when it comes to EBA and ESMA. Both EBA and ESMA are empowered to adopt technical standards in relation to specific regulations or directives which are binding for all EU Member States, as well as non-binding soft-law documents like guidelines, recommendations, opinions and reports that serve as useful sources of information not only for the regulators.

* * *

Endnotes

1. Available at: https://www.cnb.cz/export/sites/cnb/en/public/galleries/media_service/conferences/speeches/download/tomsik_20180907_sochi.pdf, p. 3.
2. Press release available at: <https://www.czech-ba.cz/cs/media-servis/tiskove-zpravy/>

- projekt-sonia-bankovni-identita-jako-nova-digitalni-obcanka-pro-sluzby-statu-i-soukromych-firem.
3. Available at: https://www.czech-ba.cz/sites/default/files/cobs_rulebook_v02.0-final_vnejsi_web.en_.pdf.
 4. EBA: <https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf>. ESMA: https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.
 5. The term “transferable security” has the same meaning as in MiFID2.
 6. The term “investment instruments” imitates the term “financial instruments” in MiFID2 without relevant changes, and as such they may be understood interchangeably in this chapter.
 7. Also DĚDIČ, J. *et. al. Proč podle českého soukromého práva nelze uvažovat o (ICO) tokonech jako cenných papírech*. Právní rádce, 15-16/2018, p. 554–556.
 8. Available at: https://www.cnb.cz/export/sites/cnb/cs/casto-kladene-dotazy/.galleries/stanoviska_a_odpovedi/pdf/k_obchodovani_s_prevodnimi_tokeny.pdf.
 9. Pursuant to Section 2(1)(l) of the AML Act, virtual currency means an electronically stored unit, whether or not it has an issuer, and which is not a payment instrument under the PSA, but is accepted as payment for goods or services by another person different from its issuer.
 10. More information is available at: <https://www.roklen.cz/roklenfx/jak-to-funguje>.
 11. Available at: https://www.cnb.cz/export/sites/cnb/en/public/.galleries/media_service/conferences/speeches/download/tomsik_20180907_sochi.pdf, p. 8.
 12. *Ibid.*
 13. See, e.g.: <https://www.lupa.cz/aktuality/axa-v-cesku-spousti-chatbota-pro-messenger-sjedna-vam-cestovni-pojisteni/>.
 14. More information is available at: <https://www.mujdok.cz/>.
 15. More information is available at: <https://pojistenafaktura.cz/#jak-to-funguje>.
 16. More information is available at: <https://www.cnb.cz/cs/dohled-financni-trh/>.
 17. The CNB’s Report on performance of supervision on the financial market, 2017.
 18. <https://www.cnb.cz/cs/cnb-news/tiskove-zpravy/Agendou-FinTech-se-bude-v-CNB-zabyvat-sekce-regulace-a-mezinarodni-spoluprace/>.
 19. https://www.cnb.cz/export/sites/cnb/cs/verejnost/.galleries/pro_media/konference_projevy/vystoupeni_projevy/download/mora_20181011_bankovni_forum.pdf.
 20. https://ec.europa.eu/info/sites/info/files/180308-action-plan-fintech_en.pdf.
 21. <https://www.cnb.cz/cs/dohled-financni-trh/vykon-dohledu/mezinarodni-aktivity/>.
 22. <https://www.uouu.cz/dozorova-cinnost/ds-1277/p1=1277>.
 23. <https://www.ilaw.cas.cz/uvod/aktuality/regulatory-sandboxes.html>.
 24. <https://www.cnb.cz/en/public/media-service/speeches-conferences-seminars/speeches/balancing-fintech-opportunities-and-risks-implementing-the-bali-fintech-agenda/>.

**Petr Vybíral****Tel: +420 222 107 173 / Email: petr.vybiral@allenovery.com**

Petr specialises in capital markets and banking and finance. He has extensive experience in representing various parties (including underwriters, dealers and issuers) on a wide range of capital markets and financing transactions, involving debt, equity and derivatives and structured finance instruments. He is also a member of the Appeals Committee of the Czech National Bank and is well-known for his unique expertise in the field of covered bonds and other types of secured financings. Petr has also advised major financial institutions and corporations on the securities and capital markets regulations in the Czech Republic and assisted in the preparation of their standard documentation for securities and derivatives. In the area of banking and finance, he has further participated in various types of acquisition and real estate financings. Petr has been recognised as a leading or recommended lawyer for capital markets in the Czech Republic in *Chambers*, *The Legal 500* and *IFLR1000*.

**Tomáš Kirner****Tel: +420 222 107 118 / Email: tomas.kirner@allenovery.com**

Tomáš specialises in financial regulation and capital markets. He has participated in the preparation of public and non-public issuances of bonds and structured certificates, and in the preparation of standard framework documentation for trading derivatives and other structured products for the Czech Banking Association. Tomáš also focuses on regulation of derivatives and represents clients in the negotiation of terms of OTC derivatives agreements. He has been advising both banking and non-banking clients in launching new financial products on the Czech market.

Allen & Overy (Czech Republic) LLP

V Celnici 4, Prague 11000, Czech Republic
Tel: +420 222 107 111 / URL: www.allenovery.com

France

Hubert de Vauplane & Victor Charpiat
Kramer Levin Naftalis & Frankel LLP

Approaches and developments

There have been significant developments in global approaches to the regulation of Fintech in recent years with new opportunities, risks and challenges for market participants, customers and regulators arising from Fintech.

Such areas of Fintech could include electronic payments, “robo advice”/algorithmic-based advice, trading and lending platforms, cryptocurrencies and related initial coin offerings/token-generating events and other blockchain technology-based applications.

In the last few years, France has jumped into the race to become Europe’s top Fintech jurisdiction. Although France cannot boast any world-scale Fintech “unicorn”, the scene is very active and a lot of promising startups were born or reached a significant scale in the last few years. French Fintech startups are supported by a strong network of business angels, venture capital funds, and professional organisations and associations. In addition, established financial institutions have adopted an open stance regarding Fintech. Some of them have created Fintech or Insurtech incubators, and most of them regularly establish business partnerships with startups. Buyouts of Fintech startups by large banks or insurance companies are also frequent.

France does not have *per se* an approach regarding Fintech regulation. Fintech, “*the term used to describe the impact of new technologies on the financial services industry*” (according to the European Commission), is not a legal notion. Fintech is firstly understood as an “umbrella term” covering various innovative business models related to the broader financial sector. Therefore, in France, the regulation to which a Fintech company may be subject depends on its activities. Whether a company self-identifies as a Fintech company has no legal impact. Still, both legislators and regulators (the *Autorité des marchés financiers* or “AMF” – the financial markets authority, and the *Autorité de contrôle prudentiel et de régulation* or “ACPR” – the banking and insurance regulatory authority) have adopted a welcoming attitude. There is a shared agenda towards improving France’s position on the global Fintech scene and establishing France as the leading European Fintech hub, in the wake of the United Kingdom’s exit from the European Union.

During the last few years, the AMF and the ACPR have launched multiple Fintech initiatives, such as the Fintech Forum in July 2016 (a consultative body gathering representatives from Fintech startups and financial institutions), the creation of internal Fintech teams acting as “innovation hubs” in 2016, or the creation of the Universal Node to ICO’s Research & Network (“UNICORN”) in October 2017 by the AMF, a taskforce dedicated to initial coin offerings (“ICOs”).

On the legislative side, first of all, it is worth noting that most of French financial and banking law derives from EU directives and regulations. As the EU legislative process is rather slow,

emerging Fintech-related trends often find themselves “unregulated”. Therefore, France regularly makes the first move and initiates the regulation of these emerging trends at the national level. For example, France passed a framework regulating crowdfunding and crowdlending in 2014, while the European Commission only issued the first proposal of its regulation on European crowdfunding service providers on March 2018. Similarly, during the first half of 2018, France decided to include a regulation of ICO issuers and crypto-assets service providers in the draft bill nicknamed “*Loi Pacte*” (which stands for “Action Plan for the Growth and Transformation of Companies”). The EU authorities, on the other hand, are still conducting preliminary consultations and assessing the need to legislate on ICOs and crypto-assets at the EU level.

Recent, impending or proposed changes to the Fintech-related regulatory architecture in France

While, as stated above, most of the French legislation applicable to financial markets and banking and payment services derives from EU directives or regulations, three recent or impending Fintech-related reforms are worth mentioning.

First, France created in 2014 a comprehensive legal framework for crowdfunding and crowdlending activities. Crowdfunding transactions up to €2.5 million are now exempted from the obligation to publish a prospectus while, before, issuers willing to raise over €100,000 in equity or bonds were subject to these requirements. In addition, the 2014 reform also introduced a new exemption from the banking monopoly (*i.e.* the rule prohibiting entities other than licensed banks from granting interest-bearing loans) allowing individuals to grant loans through crowdlending platforms. Crowdfunding and crowdlending platforms have to register with the ACPR and/or the AMF either as crowdfunding/crowdlending intermediaries (for donations and crowdlending platforms) or as crowdfunding investment advisors (for investment-based crowdfunding).

Then, with Ordinance No. 2017-1674 of 8 December 2017 and Decree No. 2018-1226 of 24 December 2018, the French government introduced innovative legislation allowing blockchain technology to be used to issue, register and transfer unlisted securities. The distributed ledger used to register securities must comply with four main technical conditions: (i) the integrity of the information recorded must be preserved; (ii) the distributed ledger must allow the identification of the owners of the securities, and the nature and number of securities held; (iii) a continuity plan including an external data recording system must be set out; and (iv) the owners of the securities registered on the distributed ledger must be able to access their statements of transactions. This legislation does not specify which of the issuer or its service provider will be responsible for the compliance of the distributed ledger with these technical requirements. The distinction between private and public blockchains is not addressed either. Complying with some of these technical requirements could be more complicated when a public blockchain is used.

Finally, the major impending Fintech-related legislation is the *Loi Pacte*. The *Loi Pacte* was discussed at length by both chambers of the Parliament, and was finally adopted on 11 April 2019 by the *Assemblée nationale*. It is expected that the *Loi Pacte* will be enacted in May or June 2019.

This bill contains a patchwork of measures aimed at facilitating the growth of small and medium-sized enterprises (“SMEs”) and giving employees and stakeholders more control over corporations. More importantly, the *Loi Pacte* introduces a comprehensive regulatory framework for ICOs and crypto-assets service providers. (This new framework will not apply to tokens which share the same characteristics as financial instruments: the offerings

of “security tokens” will have to comply with existing regulations.) With respect to ICOs and cryptocurrencies, the *Loi Pacte* contains three key measures:

- **Optional AMF approval for ICOs.** The AMF will grant an approval (“*visa*”) to public offerings of tokens. This approval will be optional and not mandatory: potential token issuers will be free to require the AMF’s *visa* or proceed with their ICO without the AMF’s approval. The AMF expects that the most serious projects will require its approval as the global reputation of the AMF would help token issuers market their ICO in other jurisdictions, as well as allow them to freely sell their token to French investors. The approval may be granted if the token issuer complies with the following requirements: (i) the issuer is a legal entity incorporated in France, or at least registered in France through a branch; (ii) the disclosure document (*i.e.* the white paper) and the marketing materials are accurate, written in plain language, non-misleading, and describe the risks associated with the offer; and (iii) the issuer plans to implement adequate procedures to track and safeguard the funds raised in the ICO.
- **Digital assets service providers.** The *Loi Pacte* will create a new category of regulated entities: digital assets service providers (*prestataires de services sur actifs numériques*). The definition of digital assets covers ICO tokens as well as other types of crypto-assets. The services related to digital assets include various kinds of traditional investment services, as soon as they are performed in relation to digital assets: (i) custody of digital assets or cryptographic private keys for third parties; (ii) purchase or sale of digital assets against legal currency (*i.e.* fiat); (iii) purchase or sale of digital assets against other digital assets; (iv) operation of a digital assets trading platform; and (v) various other services related to digital assets: receipt and transmission of orders on behalf of third parties, asset management, investment advices related to digital assets, underwriting, and placing with or without a firm commitment. This framework will also be partially optional. Only digital assets custodians and entities allowing the purchase or sale of digital assets against legal currency will have to be mandatorily registered, while the entities carrying out all the other activities may apply for an optional licence. Anti-money laundering requirements will apply to both (i) registered digital assets custodians and entities allowing the purchase or sale of digital assets against legal currency, and (ii) other digital assets service providers which obtained the optional licence.
- **Right to open a bank account.** Banks will have to set up objective, non-discriminatory and proportionate rules to determine that the following categories of entities should be allowed to open an account in their books: (i) token issuers which have been granted an optional approval by the AMF; (ii) registered digital assets service providers; and (iii) digital assets service providers which obtained the optional licence. The provision adds that their access to basic banking services shall not be hindered by the bank once the account is open. These provisions will create a strong incentive for crypto-assets issuers and intermediaries to obtain an optional *visa* or an optional licence from the AMF instead of remaining unregulated, as the right to access bank accounts will be tied to such approval or licence.

Fintech offering in France

Overview of technologies and applications, and existing or new laws and regulations

Various disruptive technologies are being applied to the finance and insurance industries by both startups and established institutions in France. Not all of these business models require a regulated status or trigger the application of specific legislation. The main Fintech-related

business models and their associated legislation are presented below (please note that other regulatory regimes may apply depending on the particularities of each business model):

- **Mobile payment apps** (e.g. Lydia, Pumpkin, Paylib): these apps allow individuals and companies to send payments directly from their mobile, without having to use their banking app. Mobile payment apps generally integrate additional payment methods (e.g. Apple Pay, QR codes, etc.) and allow their users to monitor their expenses. These companies generally partner with regulated payment service providers to comply with the regulatory requirements which would normally apply to their activities.
- **Crowdfunding and crowdlending platforms** (e.g. October, Wiseed, Anaxago, Younited, Unilend, Lendopolis): these platforms allow individuals (and, increasingly, some investment funds) to fund projects initiated by SMEs. Crowdfunding platforms allow investors to invest in the companies themselves, through the issuance of shares or bonds, while crowdlending platforms allow their users to grant loans. French crowdfunding and crowdlending platforms have been struggling recently as traditional banks are increasingly willing to lend to SMEs at low rates. In October 2018, crowdlending pioneer Unilend filed for bankruptcy. Platforms are now focusing on promising markets such as real estate and renewable energy infrastructure financing. As described above, crowdfunding and crowdlending platforms have been subject to an *ad hoc* regulatory regime since 2014. Crowdfunding and crowdlending platforms may only be operated by licensed entities, although the requirements to obtain this licence are less stringent than those generally applied to investment services providers.
- **Group gifting/personal fundraising platforms** (e.g. Leetchi, LePotCommun): these companies allow their users to collect money from friends and family to finance gifts or common projects, through the creation of an online money pot. These platforms are also increasingly used to support humanitarian causes (e.g. money pots may be organised to help a low-income family afford a costly surgical intervention, even though most contributors would not know directly the beneficiary of the money pot). Although their business models are similar, Leetchi and LePotCommun do not share the same regulatory status. Leetchi is registered as a crowdfunding intermediary (*intermédiaire en financement participatif*), a status which allows the operation of a platform through which individuals may grant loans or donate directly to fund projects. On the other hand, LePotCommun is registered as an intermediary in banking transactions and payment services (*intermédiaire en opérations de banque et en services de paiement* or “**IOBSP**”).
- **Bank accounts aggregators and personal finance apps** (e.g. Bankin’, Linxo, Budgea, Budget Insight): these apps allow their users to monitor their budget and their savings by aggregating all the accounts opened in their name (e.g. bank accounts, savings accounts, retirement accounts, securities accounts, etc.). These companies rely on the “open banking” trend which supports the right for third-party providers to access clients’ bank accounts. Most of these companies obtained a licence from the ACPR following the adoption of Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market (“**PSD 2**”) which added the account information and payment initiation services to the list of regulated payment services.
- **Neobanks** (e.g. Shine, Qonto): these companies allow their users to open bank accounts and access basic banking services (such as using a debit card and transferring funds) through a mobile app. Shine and Qonto both focus on freelancers and small companies. Although these neobanks allow their clients to open bank accounts and use debit cards,

they are not regulated as credit institutions, because their business model does not involve granting loans. Qonto was granted a payment institution licence by the ACPR, while Shine is registered with the ACPR as the agent of a regulated payment service provider.

- **Robo-advisors** (e.g. WeSave, Advize, Yomoni, Marie Quantier): robo-advisors are personalised online savings management services that allow individuals to invest their savings in a smart and automated way. Although their business models vary significantly, these companies generally rely on artificial intelligence to suggest an optimal asset allocation, which may vary over time based on the risk profile of the client and their personal savings goals. Most of these robo-advisors are primarily regulated by the AMF as financial investment advisors. Marie Quantier and Yomoni are also regulated by the ACPR as insurance brokers. Yomoni is the only robo-advisor regulated as an investment management company.
- **InsurTechs** apply innovative technologies to the insurance sector. Various business models have emerged (see below). Generally speaking, InsurTech companies are subject to the same legislation as insurance undertakings, unless they merely provide technological services to regulated entities.
- **Factoring and short-term financing providers** (e.g. Finexkap): Finexkap provides financing to SMEs through factoring (i.e. buying invoices at a discount). Finexkap improves the traditional factoring process by using machine learning, big data, and integrated APIs. Finexkap is regulated by the AMF as an investment management company and manages the securitisation fund (*fonds commun de titrisation*) which purchases the invoices.
- **ICO issuers and cryptocurrency-related companies** (e.g. Ledger, LGO, Coinhouse, Paymium, Domraider, NapoleonX, etc.): although all these companies are part of the same subcategory, their business models are very different. Ledger sells hardware wallets, LGO and Paymium operate cryptocurrencies exchange platforms, Coinhouse acts as a broker-dealer, Domraider raised funds in an ICO to develop a blockchain-based auction system, etc. Some of them are already subject to regulatory requirements: exchange platforms receiving fiat deposits from their clients must obtain a payment service provider licence from the ACPR or partner with a regulated payment service provider. In addition, these platforms are subject to anti-money laundering requirements. The regulatory status of these companies will be materially modified when the *Loi Pacte* is passed into law, as described above.
- Finally, since 2015 and 2016, most French financial institutions have started to work on implementations of **blockchain technology**. Several French banks have joined the R3 consortium which develops the private blockchain platform named Corda. Euronext, BNP Paribas, Société Générale, CACEIS, and Caisse des Dépôts have jointly created LiquidShare, a startup aimed at building a blockchain-based settlement system for non-listed securities. In addition, various major French non-financial companies are also experimenting with blockchain technology in their own field: for example, Carrefour is partnering with IBM to develop a blockchain-based food traceability platform. The French Central Bank itself developed a blockchain-based system to manage SEPA creditor identifiers.

Regulatory and insurance technology

RegTech

RegTech is a fast-expanding sector within the broader French Fintech industry. The AMF

and the ACPR strongly support the RegTech ecosystem, as RegTech is seen as both a means to help financial institutions comply with an ever-increasing amount of regulatory requirements, and a tool to help regulatory agencies to handle the vast amount of data collected pursuant to their supervision mission (nicknamed “SupTech” – supervision technology).

However, France does not appear to foster big RegTech startups. No significant fundraising related to RegTech startups has been recorded in the last few years. The association France Fintech published in February 2019 a white paper on the state of RegTech in France, which lists more than 20 French RegTech startups. Most of these companies offer products relating to the client identification process (also known as KYC) or electronic signatures.

It is also worthwhile to note that LaBChain, a blockchain innovation lab launched by the Caisse des Dépôts with various large financial institutions, started working in July 2016 on a business case dedicated to the use of blockchain to manage digital identity and KYC.

InsurTech

The major French insurers have all launched internal projects aimed at better integrating technology in their activities. Most of these projects revolve around using technology to reach potential or current customers or using data analysis to better understand their needs. Their goal is to simplify and streamline the key steps of the insurance process: quotation; subscription; payment of premiums; and payment of claims.

In addition to this gradual integration of technology, some French insurers also started specific InsurTech-related projects. Axa, the leading French insurance company, launched in 2015 Kamet, an Insurtech incubator “dedicated to conceptualising, launching and accompanying disruptive InsurTech products and services”. In 2017, Axa launched Fizzy, a flight delay insurance product built upon the Ethereum blockchain. Fizzy leverages blockchain technology to provide automatic compensation if the flight is more than two hours late, without requiring the policyholder to formally request the payment of the claim. In March 2019, Axa partnered with Assurely, a U.S. startup, to launch “CrowdProtector,” an insurance product dedicated to equity crowdfunding and security tokens issuers and investors. According to Assurely’s website: “[i]ssuers get protection against investor complaints and lawsuits. Subject to the policy’s terms, investors can get their principal investment returned should the issuer misuse the funds, purposefully misrepresent information in their offering documents or steal the money.”

Axa is not the only established financial institution dedicating resources to InsurTech. Société Générale, France’s third biggest bank, launched Moonshot-Internet, an internal startup specialised in the emerging insurance needs of Internet retailers. Société Générale also supports Chainly, which dematerialises the car insurance claim process through a chatbot.

Another noteworthy initiative is the trial of a blockchain-powered system to exchange secure data by 14 French insurers in November 2017, led by the French Insurance Federation.

Independent InsurTech startups are also thriving in France. Alan, which sells user-friendly health insurance products to startups and freelancers, raised €40 million in February 2019, after a €23 million funding round in 2018. Alan obtained a licence from the ACPR in 2016. In March 2019, Shift Technology, which specialises in fraud detection and claims automation, raised €53 million.

Regulatory bodies

French financial institutions are regulated by both the AMF and the ACPR (which is the regulatory arm of the French Central Bank). The AMF’s primary purpose is to protect

investors by ensuring the proper functioning of financial markets, while the ACPR is in charge of preserving the stability of the financial system and supervising the banking and insurance sectors.

Whether a Fintech company is subject to the supervision of the AMF or the ACPR depends on the services provided by such company. Some actors only deal with one regulator (*e.g.* a bank or an insurance company would normally only be under the supervision of the ACPR) but, in practice, most financial institutions deal with both regulators. For example, an insurance company would be regulated by the ACPR with respect to its insurance activities, but its asset management business would be subject to the AMF's supervision.

The AMF and the ACPR may also share their competences with respect to the authorisation process. For example, the ACPR is responsible for the authorisation of investment services providers, but their "programmes of activity" (*i.e.* the description of the activities carried out by the entity) must be approved beforehand by the AMF. Once investment services providers have obtained the licence, the ACPR monitors their activity and financial situation, while the AMF monitors their compliance with the applicable code of conduct.

Key regulations and regulatory approaches

France generally tries to gather all the laws related to the same industry within a single code – which may contain dozens of sections and hundreds of pages. Pursuant to this "codification" approach, most of the French financial and banking law is contained in the Monetary and Financial Code (*Code monétaire et financier*), rather than in individual bills. The Monetary and Financial Code contains a "legislative" and a "regulatory" section. The rules contained in the legislative section tend to be broad definitions, while the regulatory section generally contains detailed descriptions of the applicable regimes. At an increasingly detailed level, rules may be contained in specific regulations prepared by the regulatory authorities themselves, such as the General Regulation of the AMF or the Order of 3 November 2014 regarding the internal control of banks, payment service providers, and investment services providers subject to the supervision of the ACPR. Therefore, a Fintech startup wishing to identify the regulation to which it is subject should primarily check if an EU regulation covers its activities, and then browse the Monetary and Financial Code and identify the relevant subsections (if any).

More specifically, below is the key Fintech-related legislation applicable in France:

- Payment service providers are subject to PSD 2 and its transposal into French law.
- Banks and financial institutions are mostly subject to the CRD IV package and PSD 2, and their transposal into French law. Part of the regulation applicable to French financial institutions may differ from EU law with respect to certain specific aspects, such as the banking monopoly.
- Insurance companies are mostly subject to the Solvency II and Insurance Distribution Directives, and their transposal into French law.
- Crowdfunding and crowdlending platforms are respectively subject to Articles L. 547-1 *et seq.* and L. 548-1 *et seq.* of the Monetary and Financial Code, unless they are managed by an investment services provider.
- Investment management companies and other investment services providers are subject to a wide set of provisions of the Monetary and Financial Code and the General Regulation of the AMF, which partly derive from MiFID II.
- Companies whose business models revolve around the use of crypto-assets will be subject to the provisions of the *Loi Pacte* once it is passed into law.

Supra-national regulatory regimes or regulatory bodies

The major part of French financial and banking law directly derives from the directives and regulations elaborated by the European Commission. The European supervisory agencies (“**ESAs**”) (ESMA for financial markets, EBA for banking activities, and EIOPA for insurance activities) then elaborate delegated regulations and directives which supplement the regulations and directives on specific aspects and are later adopted by the European Commission. The ESAs are also empowered by the directives or regulations to prepare draft regulatory technical standards (“**RTS**”) and draft implementing technical standards (“**ITS**”). Then, the ESAs generally issue guidelines and question and answers (“**Q&As**”) regarding certain aspects of the EU legislation. The goals of these guidelines and Q&As is to ensure consistency in the application of the legislation. The EU legislation is then implemented at the national level by the national government and regulatory authorities.

Other supra-national regulatory regimes may also shape EU banking and financial law (e.g. the measures adopted by the Basel Committee on Banking Supervision or the recommendations issued by the Financial Action Task Force), but they would not directly influence French banking and financial law. The recommendations or measures adopted by these supra-national bodies are first included in EU law by the European institutions, before starting to apply in France.

Regulatory authorities’ commitment to Fintech

As described above, French lawmakers show an undeniable commitment to make France a leading Fintech hub. Major Fintech-related legislation include the regulation of crowdfunding and crowdlending in 2014 and the law allowing blockchain technology to be used to register and transfer unlisted securities, as well as the impending *Loi Pacte*.

On the regulatory authorities’ side, the AMF and the ACPR launched in July 2016 the Fintech Forum, a consultative body gathering representatives from Fintech startups, financial institutions, lawyers and consultancy firms. The French cybersecurity agency (“**ANSSI**”), the French data protection authority (“**CNIL**”) and the French financial intelligence unit (“**TRACFIN**”) are also associated with the Fintech Forum. In addition, in June 2016, both the AMF and the ACPR set up internal Fintech teams (the *division Fintech, Innovation et Compétitivité* at the AMF and the *Pôle FinTech Innovation* at the ACPR). These teams act as “innovation hubs”, i.e. dedicated points of contact for startups and financial institutions raising enquiries on Fintech-related issues and seeking non-binding guidance on the conformity of their products with regulatory requirements. In October 2017, during the ICO boom, the AMF also created the dedicated taskforce UNICORN.

Finally, French regulatory agencies do not plan to establish any regulatory sandbox for the time being. They favour an approach based on proportionality: although a Fintech startup would be subject to the same rules as an established financial institution, the enforcement of these rules would depend on the size of the entity and the level of risk associated with its activities. In addition, the dedicated Fintech teams of the AMF and the ACPR will provide advice and guidance to Fintech startups.

General attitudes to Fintech

The mainstream use of the concept of Fintech in France is rather recent. For example, the term “Fintech” was first used in the 2014 annual report of the ACPR. The last annual report of the ACPR still mentions the emergence of Fintech business models as a “risk”, but the overall tone is very positive.

Technology-enabled financial innovation has never been hindered *per se* in France. Therefore, the attitude concerning Fintech has not shifted; rather, Fintech emerged as a

buzzword in the last few years, and both the lawmakers and the regulatory authorities launched initiatives to strengthen France's position in the global and European Fintech ecosystem. Although France is certainly not as advanced as certain European jurisdictions, such as Malta, Liechtenstein, the United Kingdom and the Baltic countries, many efforts have been made and continue to be made in order to develop an innovation-friendly Fintech regulation in France. The *Loi Pacte*, in particular, is a notable effort to take the lead with respect to the regulation of ICOs and crypto-assets.

Finally, in April 2019, France hosted the Paris Blockchain Week, a week-long event dedicated to blockchain technology and crypto-assets. The event was introduced by a conference organised by the Ministry for the Economy and Finance, during which members of the government reaffirmed their goal to turn France into a leading jurisdiction for blockchain technology.

Restrictions

To our knowledge, there are no specific restrictions regarding Fintech activities in France. The only restriction is that regulated activities must be carried out by regulated entities. However, the process of obtaining an authorisation from the ACPR or the AMF is generally long and costly, which prevents many Fintech startups from developing certain business models, as soon as part of their business model is subject to the regulator's authorisation.

The main incentive not to engage in certain activities relates to cryptocurrencies. Although the AMF or the ACPR have not issued specific recommendations on the matter, it is highly likely that they would discourage any large financial institution trying to create an internal cryptocurrency-related business without having it ring-fenced in the first place. Being exposed to the volatility risk of cryptocurrencies would probably not be well perceived by the ACPR or the AMF. Otherwise, the involvement in Fintech is generally well perceived by the French regulatory authorities.

To our knowledge, the development of Fintech in France has not created any significant disruption. The development of cryptocurrencies, however, has prompted the AMF and the ACPR to issue joint statements warning individual investors against the risks of investments in cryptocurrencies.

Cross-border business

Most French Fintech startups only address the French market. However, as they grow and raise funds, some of these companies expand into other EU countries. EU law encourages this expansion with the European passport system: entities licensed in a European Economic Area ("EEA") Member State may provide regulated services on the territory of another EEA Member State either through a branch or subsidiary (freedom of establishment) or directly, without permanent establishment (freedom to provide services).

These passporting rules also allow foreign Fintech startups to offer regulated services in France after having obtained a licence from the regulatory authority of any EU country, including "small" ones. For example, neobank Revolut obtained in December 2018 a banking licence from the Bank of Lithuania. Some worry that the regulatory agencies of these small EU countries may engage in a form of regulatory dumping by offering Fintech startups a "fast-track" payment or banking licence. The licensing process of the Bank of Lithuania is reportedly as short as three months, while obtaining the same licence in France may take between six and 12 months.

To our knowledge, no French startup has used this strategy to accelerate its growth. However, various Fintech startups (in particular those active in the blockchain industry) find themselves compelled to partner with entities regulated in small EEA countries (such as Liechtenstein), because French banks are reluctant to work with them.

Cross-border collaboration with global regulators

The AMF and the ACPR are involved in supranational working groups regarding various Fintech-related issues. For example, the ACPR is a member of the Committee on Consumer Protection and Financial Innovation (organised by the EIOPA) and the Standing Committee on Consumer Protection and Financial Innovation (organised by the EBA), the latter of which notably focus on the risks associated with crowdfunding and crypto-assets. Generally speaking, the AMF and the ACPR extensively participate in the Fintech-related working groups organised by the ESAs.

In addition, the AMF and the ACPR have both established Fintech-related partnerships with various non-EU regulatory agencies. The ACPR partnered with South Korea, Japan, and Singapore, while the AMF has sealed Fintech-related agreements with the regulatory agencies of China, Singapore, the United Arab Emirates, and Mauritius.

Regarding the global financial regulation, the AMF is also involved in the Fintech-related working groups organised by the Financial Stability Board, the International Organization of Securities Commissions, and the Committee on Payments and Market Infrastructures.

**Hubert de Vauplane****Tel: +33 1 44 09 46 80 / Email: hdevauplane@kramerlevin.com**

Hubert de Vauplane co-leads the Alternative Investment Management practice in the Paris office, offering a global and integrated vision on regulatory and transactional structuring and operations matters. Hubert advises on EU and French laws on banking and investment services regulatory matters, asset management and funds, insurance investment regulations, and financial/securities litigations, e-money and payment services, and financial institution mergers and acquisitions. He provides legal counsel on fintech, blockchain and cryptocurrency assets, and financial regulatory issues relating to investment advice, asset management, payment services and banking.

Hubert also advises corporates, asset managers, corporate and investment banks and institutional investors in relation to the entire range of disintermediated financings, including the structuring and setting-up of debt funds (AIFM, ELTIF, FPE) under French or Luxembourg law, factoring programmes of trade receivables (French or pan-European), and the issuance of private bonds and hybrid debt instruments (EuroPP, USPP, *bons de caisse*).

**Victor Charpiat****Tel: +33 1 44 09 46 75 / Email: vcharpiat@kramerlevin.com**

Victor Charpiat's practice focuses on financial market regulations, as well as the regulation of fintech, blockchain and cryptocurrencies. Victor also advises French and foreign financial institutions with respect to financial services (notably, the marketing of financial products, investment services and post-market regulation) and other financial market transactions (credit loans, bond issuances, Euro PP, ICOs).

Kramer Levin Naftalis & Frankel LLP

47 avenue Hoche, 75008 Paris, France
Tel: +33 1 44 09 46 00 / URL: www.kramerlevin.com

Germany

Dr. Alexander Behrens, Dr. Stefan Henkelmann & Kai Schadtler
Allen & Overy LLP

Approaches and developments

Approaches to FinTechs in German law and regulatory practice

The FinTech phenomenon is gathering considerable momentum both nationally and internationally. Regulators address this phenomenon in different ways, depending on the legal framework in which they operate and the scope of their respective mandates. German regulatory law follows a principle-based and technology-neutral approach to FinTechs. Whether and to what extent FinTechs are regulated depends on the business model they follow, based on the principle “same business, same risks, same rules”.¹ That means, once a FinTech has entered regulated territory, it will be supervised by the Federal Financial Supervisory Authority (*Bundesanstalt für Finanzdienstleistungsaufsicht* – “**BaFin**”) in the same way and according to the same rules as established institutions. However, BaFin also stresses that it applies “proportionate” supervision (i.e. small businesses with low-risk positions are supervised differently from large businesses with high-risk positions). BaFin has no mandate to promote innovation or stimulate economic development in certain financial sectors, unlike regulators in other jurisdictions may have. For example, the UK Financial Conduct Authority is committed to encouraging innovation in the financial sector, which has led to the launch of Project Innovate in 2014 to provide, among other things, support for innovative firms who are ready to test their propositions in the market using a customised regulatory environment (“regulatory sandbox”).

The EU as a driving force for developments in the FinTech sector

Regulatory developments in the German FinTech sector are driven primarily by the European Union (“**EU**”), which has launched various FinTech-related initiatives in recent years. These are all part of the Digital Agenda for Europe, which in turn forms one of the seven pillars of the Europe 2020 Strategy.² In September 2017, following a public consultation phase,³ the EU Commission presented a package of measures aimed at increasing the convergence of licensing requirements for FinTechs through numerous amendments to EU secondary legislation.⁴ A far-reaching FinTech Action Plan followed in March 2018,⁵ a core element of which is a proposal for a regulation on crowdfunding.⁶ In addition, the main aim of the FinTech Action Plan is to monitor and support the further development of the FinTech sector; for example, by setting up a new expert group on regulatory obstacles to financial innovation and an “EU FinTech Lab” as a platform between regulators and market participants. Finally, the inclusion of virtual currencies in the fifth EU Money Laundering Directive also has an impact on FinTechs.⁷ The German legislator, on the other hand, has so far hardly reacted to innovations in the FinTech sector.

Definition of FinTechs

As omnipresent as the acronym “FinTech” is in the general media and increasingly also in

legal literature in Germany, it is difficult to define. Although it can be broken down relatively easily into its two components “financial (services)” and “technology”, the insight gained from this is limited. It is not even clear whether the term refers to the actors involved or to specific services. Regulatory practice in Germany, however, has given rise to a definition of FinTech that refers to both actors and specific services. According to BaFin, FinTechs are:

“young undertakings that provide specialised and in particular customer-oriented financial services using technology-based systems. As such, FinTechs follow the trend towards digitalisation and customisation, and encourage digital progress in the financial market at the same time. They rely in particular on customer-friendly, fast and convenient applications for the user. However, FinTechs are not just in competition with traditional financial services providers such as banks, insurers and investment firms, they also to some extent supplement the services that these offer.”⁸

Services provided by FinTechs are generally based on innovative technologies, including Big Data, artificial intelligence or distributed ledger technologies (“**DLT**”) such as blockchain, the use of which is intended to revolutionise the conventional way of providing financial services.

FinTech offering in Germany

In Germany, FinTechs cover a wide range of different business models. Many of these undertakings offer services that are similar to those provided by established institutions, such as loan brokerage (“crowdfunding”) and automated investment advice (“robo-advice”). Others supplement these traditional services with additional services, particularly in the area of payment solutions and crypto currencies. The following gives a rough overview of different business models that FinTechs are pursuing in Germany today.

Payment solutions

Technological trends in payment solutions started gathering pace in Germany at the beginning of the 21st century with the introduction of the first online payment methods. Today, providers of innovative payment solutions account for the largest share of the FinTech sector in Germany. With these new payment solutions, the use of smartphones for executing payment transactions is also becoming increasingly important (“mobile payment”). There are two types of mobile payment. Mobile “proximity” payments refer to the act of paying with a mobile device using a “proximity” technology (such as Near Field Communication (“**NFC**”), Quick Response (“**QR**”) codes, or Bluetooth) typically at the Point of Sale (“**POS**”); e.g., in a merchant store. In Germany, this type of mobile payment is offered, for example, by Apple Pay or AliPay, the latter of which is currently only available for users with a Chinese bank account. Mobile “remote” payments on the other hand are independent of the customer and merchant location and are used for online shopping from a mobile device (m-commerce), but may also be used for Person-to-Person (“**P2P**”) payments using a mobile telecommunication network (such as the Global System for Mobile Communications (“**GSM**”), or mobile internet). The underlying payment instrument of both mobile proximity payments and mobile remote payments may be a payment card, direct debit or credit transfer. As such, they do not differ significantly from established payment methods, but only make them accessible for the payer via his/her mobile device.

Innovative payment solutions also include those based on an e-wallet or digital wallet. An e-wallet is a virtual account that allows users to store and receive funds in the form of electronic money (“**e-money**”) in order to make payments. E-wallets may be used, for example, to purchase items online via a computer or in a shop using a smartphone. Typically,

e-wallets are linked to a bank account or credit card via which fiat money can be exchanged for e-money and *vice versa*. The market leader in Germany for e-wallet payment solutions is PayPal, which, with a market share of 19.9% of sales in German e-commerce, is the third most common payment method after invoices and direct debits and before credit cards. PayPal attracts users for, among other things, the customer protection associated with its payment service, according to which the buyer receives a refund from PayPal if the seller fails to meet its obligations, e.g. if the seller delivers a defective product.

Crypto currencies

A separate form of payment solution is crypto currencies. Crypto currencies are virtual means of payment created and managed in a decentralised computer network, independent from the state or a payment service provider. Technically speaking, crypto currencies are encrypted data packages which are stored in a virtual wallet. The most well-known and oldest crypto currency is Bitcoin. The Bitcoin network is based on a database jointly managed by the network participants, the so-called “blockchain”. Bitcoins can either be purchased via online trading platforms in exchange for fiat money or created by “mining”, which requires the solution of complex computational maths problems in the Bitcoin network. Since the total amount of Bitcoins is limited to 21 million by the source code, mining is becoming increasingly difficult and can only be done lucratively by computers with enhanced performance. However, Bitcoin is not the only crypto currency. Since the white paper entitled “Bitcoin: A Peer-to-Peer Electronic Cash System” was published under the pseudonym Satoshi Nakamoto in November 2008, and the first 50 Bitcoins – the so-called genesis block – were mined on 3 January 2009, numerous alternative concepts have entered the crypto currency market. Nevertheless, Bitcoin, with a market capitalisation of around USD 92.4 billion, is currently leading by a considerable margin, ahead of Ethereum with around USD 16.3 billion and Ripple with around USD 12.3 billion.⁹

In Germany, the Stuttgart Stock Exchange is playing a pioneering role, offering investors easy access to trading in crypto currencies via its app Bison. This is planned to be followed shortly by a platform for initial coin offerings (“ICOs”) and a multilateral trading facility (“MTF”) for crypto currencies. Finally, the exchange provides solutions for the safe custody of digital assets. As an established market player, the aim of the Stuttgart Stock Exchange is also to set standards that contribute to the acceptance of crypto currencies as a new asset class. In addition, the Deutsche Börse Group, operator of the Frankfurt Stock Exchange, has partnered with the telecommunications provider Swisscom and Switzerland-based FinTechs Sygnum and Custodigit AG to set up a digital asset platform intended to provide a number of solutions in the digital assets space, including issuance, custody, liquidity provision and banking services, all using blockchain technology. The first products of the crypto exchange are to be launched later this year.

Crowdfunding

The idea of crowdfunding draws directly on traditional banking business. It involves raising capital from multiple backers (the crowd) in order to provide financial support for a specific project. This often takes place via online platforms. The crowdfunding market in Germany can be divided into four sub-segments, namely:¹⁰ (i) donation-based crowdfunding, in which the backer receives nothing in return but a sense of satisfaction; (ii) reward-based crowdfunding, in which there is a prospect of symbolic remuneration, e.g. by inclusion of the backer’s name in the credits of a movie financed by crowdfunding; (iii) crowdlending, which is characterised by the repayment of the amount provided, with or without interest; and (iv) crowdinvesting, where the backer’s objective is to obtain a financial return either

by participating in the future profits of the project or by receiving equity or debt instruments of the financed company.

In particular, initiators of creative, cultural or social projects increasingly rely on donation-based or reward-based crowdfunding as an alternative or supplement to traditional forms of financing, such as loans, venture capital, business angels, or grants. For them crowdfunding is often an attractive option since there are practically no financial offerings tailored to their specific needs. One of the largest reward-based crowdfunding projects in Germany to date is the cinema adaptation of the television series *Stromberg*. In December 2011, the production company Brainpool launched a promotion website to raise funds for the movie. The intention was to raise EUR 1 million by March 2012, a goal which was achieved within a week. In contrast to the financing of creative, cultural and social projects, crowdlending and crowdinvesting are used as financing instruments by start-up companies, who are often unable to meet the requirements for conventional financial instruments, such as providing audited financial statements or collateral.

Donation- and reward-based crowdfunding represent the smallest crowdfunding sub-segment in Germany.¹¹ With project financing totalling EUR 120 million since 2007 and an average financing amount of EUR 1,600, the volume of donation- and reward-based crowdfunding is significantly lower than, for example, the financing of start-up companies through crowdinvesting. In 2016, 55 donation- and reward-based crowdfunding platforms were active on the German market and brokered project financing totaling EUR 35 million. The world market leader in donation- and reward-based crowdfunding is Kickstarter, a US company that has been active in Germany since 2015.

With corporate financing totalling EUR 180 million since 2011, crowdinvesting is the second largest crowdfunding sub-segment in Germany. By 2016, a total of 75 crowdinvesting platforms had been established in Germany, 35 of which successfully brokered at least one corporate financing. The total volume of crowdinvesting projects in 2016 amounted to EUR 70 million. The market leader in crowdinvesting is Companisto, which entered the German market in 2012. The largest crowdfunding sub-segment in Germany, however, is crowdlending. Between 2007 and 2016, loans totalling EUR 659 million were brokered by crowdlending platforms in Germany. In 2016, the total volume of the German crowdlending market amounted to EUR 294 million. The first two crowdlending platforms, eLolly and Smava, entered the German market in 2007; Auxmoney, today's market leader in crowdlending, followed soon afterwards. By 2017, a total of 15 crowdlending platforms have been established in Germany.

Robo advice

Robo advice is another business model pursued by FinTechs in Germany. The customer uses a program that provides support in financial investment decisions, i.e. without a human investment adviser. Online platforms are often used for this, whereby the potential investor enters personal data that is significant for the purposes of the investment decision. This includes, among other things, their risk appetite and the investment amount. An algorithm subsequently determines the appropriate financial instruments and the amount of their *pro rata* inclusion in the customer's investment portfolio. The composition of the portfolio and the market situation are regularly reviewed by the program. If it determines that the investment parameters envisaged for the customer are no longer being adhered to due to market developments, the program recommends (investment advice) or initiates (portfolio management) the purchase or sale of financial instruments in order to adjust the portfolio back to the specified investment parameters. Robo advisors may pursue active and passive investment and diversification strategies.

In Germany, this form of investment advice or portfolio management, respectively, was first offered in 2013 by Quirion and Cashboard. While the first company is still one of the market leaders in robo advice alongside Scalable Capital, the latter went insolvent in 2017. In 2016, 35 companies providing robo advice were active in Germany. The assets under management by these companies in 2016 totaled EUR 571 million; the average annual growth rate of assets under management by robo advisors between 2013 and 2016 was 730%.

Regulatory and insurance technology

Insurance technology

There are many different business models that FinTechs in the insurance industry (so-called “**InsurTechs**”) can adopt. They extend across all stages of the value chain of insurance products. A wide range of terminology is used in the descriptions of such business models (e.g. peer-to-peer insurance or comparison portal). However, the business models can roughly be divided into insurance undertakings and insurance intermediaries. While in Germany InsurTechs were at first predominantly active in the areas of distribution and contract management, i.e. as insurance intermediaries, the number of InsurTechs that provide insurance services themselves is steadily increasing. The InsurTechs, which act as insurance undertakings, do not only cover the areas of indemnity/casualty insurance; for example, ottonova Krankenversicherung AG, the first digital insurance undertaking in Germany, is rather a health insurer. In the field of insurance intermediation, a variety of business models also exist. These range from comparison portals with the option of concluding insurance contracts to insurance agents who act as underwriters. In these cases, the inherent risk entailed in insurance contracts is not borne by the InsurTech, but rather by an established insurance undertaking cooperating with the InsurTech. Depending on the business model of the respective InsurTech, the activity may be subject to a licensing requirement. While InsurTechs that act as insurance undertakings usually require a licence pursuant to Sec. 8(1) of the Insurance Supervision Act (*Versicherungsaufsichtsgesetz*) from BaFin, insurance intermediaries may require a licence pursuant to Sec. 34d of the Industrial Code (*Gewerbeordnung* – “**GewO**”) from the local chamber of industry and commerce (*Industrie- und Handelskammer*).¹²

Regulatory technology

Regulatory technology (“**RegTech**”) focuses on the more effective and efficient mapping, fulfillment and documentation of regulatory obligations supported by innovative technologies. As such RegTech could be relevant for a multitude of economic sectors. However, definitions of institutions such as the Financial Stability Board, the European Banking Authority and the Bank for International Settlement all define RegTech as an application of innovative financial technology by supervised institutions to meet regulatory requirements. There is no generally accepted categorisation of RegTech applications. The known use cases are continuously extended by new application possibilities. The market currently offers applications that can be used in compliance management (e.g. automated evaluations of regulatory requirements, monitoring of compliance status and gap analyses, and technically supported disclosures of shareholder structures), risk management (e.g. automated alerts and countermeasures initiated based on quantitative analysis, data-driven and automated credit review procedures, and technically supported data generation and aggregation for *ad hoc* stress tests), customer verification (e.g. technically supported background checks using alternative data sources and the use of biometric identity verification techniques), fraud detection (e.g. automated money-laundering checks, activity

and transaction monitoring using machine learning techniques) and many other areas.¹³ In general, the use of RegTech applications does not require any special licence from BaFin. However, this use must not give rise to any unreasonable risks. In any case, BaFin closely monitors developments in the RegTech sector.

Regulatory bodies

There is no special regulatory authority for FinTechs in Germany. Depending on the business model that a FinTech pursues, it is rather subject to supervision as a credit institution, investment firm, payment institution or insurance undertaking. Supervision of these types of institutions is generally carried out by BaFin together with Deutsche Bundesbank. While Deutsche Bundesbank focuses on fact-finding and data preparation (in particular on solvency, liquidity, statistics and risk management), BaFin is primarily responsible for licensing procedures as well as ongoing supervision of the institutions with the aim of enforcing compliance with the requirements laid down in the Banking Act (*Kreditwesengesetz* – “KWG”) and other laws.

Having said that, a special supervisory regime applies to credit institutions. Under the Single Supervisory Mechanism (“SSM”), credit institutions deemed “significant” are supervised directly by the European Central Bank (“ECB”), while smaller credit institutions continue to be directly monitored by BaFin. However, due to the high requirements that a credit institution must meet in order to be considered “significant”, no FinTech in Germany is subject to direct supervision by the ECB. Certain supervisory competences in this area, in particular the granting and withdrawal of licences and the assessment of change of control notifications, have been fully transferred to the ECB under the SSM. Consequently, it is the ECB which ultimately decides whether or not a FinTech wishing to conduct banking business in Germany receives a licence.

Key regulations and regulatory approaches

Licensable activities

As set out above, whether and to what extent FinTechs are regulated depends on the business model they follow. If FinTechs wish to carry out licensable activities in Germany commercially or on a scale which requires commercially organised business operations, a written licence from BaFin is required. Licensable activities include in particular banking business, financial services, payment services and e-money business. While licensing requirements for conducting banking business and the provision of financial services are contained in Sec. 32 of the Banking Act (*Kreditwesengesetz* – “KWG”), licensing requirements for the provision of payment services and conducting e-money business are laid down in Sec. 10 and Sec. 11 of the Payment Services Supervisory Act (*Zahlungsdienstenaufsichtsgesetz* – “ZAG”).

The licensable banking businesses and financial services are listed in Sec. 1(1) Sent. 2 and Sec. 1(1a) Sent. 2 KWG, respectively. In general, it can be said that the investment services and activities listed in Section A of Annex I to the Markets in Financial Instruments Directive 2014/65/EU (MiFID II) and the activities subject to mutual recognition listed in Annex I to Directive 2013/36/EU on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms (CRD IV) are licensable in Germany. The licensable payment services are listed in Sec. 1(1) Sent. 2 ZAG and comprise those activities listed in Annex I to Directive (EU) 2015/2366 on payment services in the internal market (PSD II). Finally, licensable e-money business is defined in Sec. 1(2) Sent. 2 ZAG

as the issuance of e-money. In addition to licensing requirements, the aforementioned laws as well as the Securities Trading Act (*Wertpapierhandelsgesetz*) contain conduct and organisation rules for licensed entities, which are also to be complied with by FinTechs with a corresponding licence.

Potential licensing requirements for FinTech business models

Payment solutions

Mobile payment solutions have in common the fact that they usually make use of established payment instruments, such as payment cards, direct debits or credit transfers. Most mobile payment solutions are therefore not completely new payment methods, but merely offer users a new and mobile frontend for payment handling. Whether or not a mobile payment services provider requires a licence depends on how the payment handling is executed and which contracts it is based on. In general, the following applies: if the mobile payment service provider obtains possession of client money during the payment process, it will probably require a licence for money remittance business pursuant to Sec. 1(1) Sent. 2 No. 6 ZAG. If, on the other hand, the service provider simply provides the technology, without being itself involved in the execution of the payment process (which is usually performed by a credit institution or credit card company acting as cooperation partner), it may benefit from an exemption that exists for technical service providers. What is important is that the cooperating PSP must conclude contracts with the users in relation to the provisions of the payment services. The users must be able to exercise their contractual rights with regard to the PSP. The contracts which the service provider concludes with the payment service users must be limited to technical services.

Crypto currencies

It has been BaFin's administrative practice for several years now to view Bitcoins and other crypto currencies as financial instruments in the form of "units of account" (*Rechnungseinheiten*) within the meaning of Sec. 1(11) Sent. 1 No. 7 KWG.¹⁴ Consequently, the rules for dealings in financial instruments apply. As such, just using crypto currencies as a substitute for cash or deposit money to participate in exchange transactions does not require a licence. A merchant may thus receive payment for his products or services in crypto currencies without carrying out licensable activities. The same applies to the customer. Equally, mining crypto currencies in and of itself does not trigger a licensing requirement as the "miner" does not issue or place the crypto currencies. The sale of crypto currencies, either self-mined or purchased, or their acquisition is generally not licensable. Only under additional circumstances may a commercial handling of crypto currencies trigger a licensing requirement under the KWG.

Commercial trading in crypto currencies is mostly done via crypto exchanges. These encompass a large number of different business models.¹⁵ Those buying and selling crypto currencies in their own name for the account of others carry out licensable principal broking business pursuant to Sec. 1(1) Sent. 2 No. 4 KWG. The purchase and sale of crypto currencies are made for the account of others when the economic advantages and disadvantages of that business affect the principal. If no principal broking business is carried out by platforms, they may instead be operating a MTF pursuant to Sec. 1(1a) Sent. 2 No. 1b KWG. The existence of a MTF is likely in particular in case of platforms where sellers place crypto currencies and set a price threshold above which a trade should be executed, or where sellers secure their transactions by a deposit in the form of crypto currencies that are transferred to the platform but only released after the seller has confirmed the payment. Finally, providers that act as "currency exchanges" offering to exchange legal tenders against

crypto currencies, or crypto currencies, against legal tenders, carry out dealing on their own account pursuant to Sec. 1(1a) Sent. 2 No. 4 KWG. This is the case when crypto currencies are not only mined, purchased or sold in order to participate in an existing market, but when a special contribution is made to create or maintain that market. Due to the additional service element, this then constitutes dealing on one's own account, which requires a licence.

Crowdfunding

As regards crowdfunding, the licensing requirements depend on the type of crowdfunding – donation- and reward-based crowdfunding, crowdinvesting or crowdlending. The granting of money loans in context of crowdlending may qualify as licensable lending business pursuant to Sec. 1(1) Sent. 2 No. 2 KWG. In order to avoid a licensing requirement, crowdlending platforms often cooperate with a credit institution (so-called “fronting bank”), which first grants the loan and then assigns the loan receivables either to the crowdlending platform, an intermediary or to the lenders. The ongoing purchase of loan receivables, in turn, can trigger a licensing requirement for factoring pursuant to Sec. 1(1a) Sent. 2 No. 9 KWG, but only if it is conducted on the basis of a framework agreement. If crowdlending platforms also accept funds from lenders upfront in order to hold them in safe custody until the loan agreement is concluded, this may qualify as licensable deposit business pursuant to Sec. 1(1) Sent. 2 No. 1 KWG.

The licensing requirements for crowdinvesting generally correspond to those of crowdlending. In addition, further potential licensing requirements arise for FinTechs as the operator of crowdinvesting platforms, in particular if debt instruments are issued by the company seeking capital. In this case, the crowdinvesting platform may provide licensable investment brokerage or investment advice pursuant to Sec. 1(1a) Sent. 2 Nos. 1 and 1a KWG.

Notwithstanding the above, crowdlending and crowdinvesting platforms do not require a licence under Sec. 32(1) KWG, if they benefit from an exemption pursuant to Sec. 2(6) No. 8(e) KWG. Accordingly, anyone whose financial services for others consist only of investment advice and/or investment brokerage between customers and providers or issuers of capital investments within the meaning of Sec. 1(2) of the Capital Investment Act (*Vermögensanlagegesetz – “VermAnlG”*) is exempted from the licence requirement if, in providing such financial services, he/she is not entitled to acquire ownership or possession of client money. This is generally the case with crowdlending and crowdinvesting platforms operating in Germany. Having said that, even if crowdlending and crowdinvesting platforms benefit from the exemption in accordance with Sec. 2(6) No. 8(e) KWG, they may nevertheless require a licence under Sec. 34c and/or Sec. 34f GewO, if they provide investment brokerage or investment advice on a commercial basis with regard to capital investments within the meaning of Sec. 1(2) VermAnlG.

In contrast, donation- and reward-based crowdfunding, in which the funds made available are generally non-repayable, is not subject to any licensing requirement.

Robo advice

The rendering of robo advisory services with the model described above frequently presupposes that licensable financial services are performed. Such services may include investment advice or portfolio management pursuant to Sec. 1(1a) Sent. 2 No. 1a or No. 3 KWG and, where applicable, investment or contract broking pursuant to Sec. 1(1a) Sent. 2 No. 1 or No. 2 KWG. The latter applies to service providers that are also brokering transactions on the purchase and sale of financial instruments. For the licensing requirement, it is irrelevant whether or not the service provider makes use of automated processes and

via which channel of distribution it approaches potential customers. However, there are many different ways to provide robo advice, which makes allocation to one licensable activity difficult. For this reason, BaFin stresses that the supervisory assessment depends very much on how a particular robo-advisory platform is structured and on what contractual arrangements are agreed with the users.¹⁶

Restrictions

There are no types of FinTech businesses that are generally prohibited in Germany. As set out above, German law does not provide for a general “privilege” for FinTechs under financial regulatory laws either. If a FinTech’s business model includes a licensable activity, it must obtain the relevant licence. Necessary licences may include banking licences or licences for providing financial services pursuant to Sec. 32 KWG, payment services or e-money licences pursuant to Sec. 10 or Sec. 11 ZAG and insurance licences pursuant to Sec. 8 VAG.

Cross-border business

BaFin assumes that licensable activities are carried out *in Germany* not only if the provider of the service has its registered office in Germany, but also if the provider of the service has its registered office outside of Germany and targets the German market in order to offer its services repeatedly and on a commercial basis to companies and/or persons having their registered office or ordinary residence in Germany.¹⁷ Providers from non-EEA states that wish to market licensable services or products specifically in Germany must therefore establish a subsidiary (Sec. 33(1) Sent. 1 No. 6 KWG; Sec. 12 No. 8 ZAG) or a branch (Sec. 53 KWG; Sec. 42 ZAG) in Germany in order to obtain the required licence. Companies from EEA states may conduct business requiring a licence not only by establishing a branch but also on a cross-border basis – without having a presence in Germany – (Sec. 53b(1) KWG; Sec. 39(1) ZAG), subject to the requirements of Sec. 53b KWG or Sec. 39 ZAG (so-called notification procedure/EU Passport).

However, there is no restriction on the so-called freedom to provide requested services (*passive Dienstleistungsfreiheit*), i.e. the right of persons and entities domiciled in Germany to request the services of a foreign entity on their own initiative. Transactions requested on the client’s own initiative are therefore not subject to the licensing requirements under Sec. 32 KWG, Sec. 10 or Sec. 11 ZAG (so-called reverse solicitation exemption).

* * *

Endnotes

1. BaFin, FinTech companies, 2016 Annual Report, p. 65, available at: https://www.bafin.de/SharedDocs/Downloads/EN/Jahresbericht/dl_jb_2016_en.pdf?__blob=publicationFile&v=4.
2. COM(2010) 2020 final.
3. Responses available at https://ec.europa.eu/info/consultations/finance-2017-fintech_en.
4. COM(2017) 536 final.
5. COM(2018) 109 final.
6. COM(2018) 113 final.

7. Cf. Article 1(1)(c), (2)(d) of Directive (EU) 2018/843 (OJ L 156, 20.6.2018, p. 43).
8. BaFin, FinTechs: Young IT companies on the financial market, available at: https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2016/fa_bj_1601_fintechs_en.html;jsessionid=10392FF41C937C5DE43019F0B7F8380C.1_cid372?nn=8054672.
9. Source: <https://coinmarketcap.com/> (as at 29.04.2019).
10. Cf. on the following BaFin, Crowdfunding: Supervisory requirements and investor responsibility, available at: https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2014/fa_bj_1406_crowdfunding_en.html;jsessionid=CE18CE783EEB9CF6769D366A0C8A745E.2_cid381?nn=8249098.
11. The figures set out in the following are taken from Dorfleitner *et al.*, in: Möslin/Omlor, *FinTech-Handbuch*, 2019, p. 25 *et seqq.*
12. Cf. BaFin, Insurtech Companies, available at: https://www.bafin.de/EN/Aufsicht/FinTech/Insurtech/insurtech_node_en.html.
13. The aforementioned examples are from BaFin, *Regtech auf dem Vormarsch*, available at: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2019/fa_bj_1903_Regtech.html.
14. Cf. BaFin, Guidance Notice on Financial Instruments pursuant to Sec. 1(11) Sent. 1 to 3 KWG (*Hinweise zu Finanzinstrumenten nach § 1 Abs. 11 Sätze 1 bis 3 KWG*), available at: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111220_finanzinstrumente.html.
15. The following draws on BaFin, Virtual Currency, available at: https://www.bafin.de/EN/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node_en.html.
16. BaFin, Robo-advice and auto-trading – platforms for automated investment advice and automatic trading, available at: https://www.bafin.de/EN/Aufsicht/FinTech/Anlageberatung/anlageberatung_node_en.html.
17. Cf. BaFin, Notes regarding the licensing for conducting cross-border banking business and/or providing cross-border financial services, available at: https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Merkblatt/mb_050401_grenzueberschreitend_en.html.

**Dr. Alexander Behrens****Tel: +49 69 2648 5730 / Email: Alexander.Behrens@AllenOvery.com**

Alexander advises banks and other financial service providers, including FinTech companies, as well as unregulated companies on all aspects of financial regulatory law. In addition to German and European banking regulatory law, he focuses on payment services law and capital markets regulation as well as issues related to the Banking Union. Furthermore, Alexander has broad experience in the areas of M&A of regulated entities, NPL transactions, civil banking law and in internal investigations in the finance sector.

**Dr. Stefan Henkelmann****Tel: +49 69 2648 5997 / Email: Stefan.Henkelmann@AllenOvery.com**

Stefan is a Partner at Allen & Overy LLP, Frankfurt with broad expertise advising on German and international capital markets transactions. Stefan specialises in advising on securitisations and other structured finance transactions (covering true sale, secured loan and synthetic structures and alternative lending across a broad range of asset classes), derivatives and financial market infrastructure (such as clearing of securities and OTC derivatives), FinTech products as well as restructurings in the capital markets sector. Another focus of his practice is providing advice on bond transactions including *Pfandbriefe*, covered bonds, structured notes, hybrid and corporate bonds. Stefan has broad experience in advising on all related regulatory and insolvency law matters.

**Kai Schadtler****Tel: +49 69 2648 5768 / Email: Kai.Schadtler@AllenOvery.com**

Kai is a member of the International Capital Markets team in the Frankfurt office of Allen & Overy. He advises banks and other financial services providers, including FinTech companies, on all aspects of financial regulatory law, with a particular focus on payment services law, capital markets regulation and German and European banking supervisory law. In addition, Kai has broad experience in the areas of retail and electronic banking, M&A of regulated entities as well as anti-money laundering law.

Allen & Overy LLP

Bockenheimer Landstraße 2, 60306 Frankfurt am Main, Germany
Tel: +49 69 2648 5000 / URL: www.allenoverly.de

India

Shilpa Mankar Ahluwalia & Himanshu Malhotra
Shardul Amarchand Mangaldas & Co

Approaches and developments

FinTech has caused significant disruption in payments and lending in India. Rapid developments in mobile and telecommunications technology coupled with the Indian Government's incentivised support for digital payments have led to tremendous innovation and growth of FinTech products.

In the digital payments space, mobile pre-paid wallets had initially captured a significant share of the stored value digital payments market. The ease of access and compatibility with several online and offline platforms contributed towards their seamless use by customers for purchase of a wide set of goods and services. The stored pre-paid wallet space was initially dominated by non-bank players in the country, but banks were quick to sense the potential that this space has to offer, and proceeded to launch pre-paid wallets on their own as well as by entering into partnerships and other collaboration arrangements with technology partners. Changes in law (particularly around KYC and onboarding of customer rules), however, have significantly increased the regulatory burden and costs of operation for wallet players, causing several of them to re-think their business strategy. The United Payments Interface (“UPI”) enabled payment solutions (also discussed in more detail subsequently) today have the most use case in the payments landscape.

Banks and non-bank players initially launched competing FinTech products and the FinTech landscape in India was, for a while, segmented into bank vs. non-bank players. The market has, however, shifted to a more collaborative model, with banks and non-bank entities partnering on several dimensions, each leveraging their respective strengths to provide customers easy-to-use financial products. Non-banks have the ability to leverage technology more effectively and are able to access customers and markets that banks would find too expensive to tap in the ordinary course. Banks have strong balance sheets and a good understanding of the regulatory and licensing regime governing financial products.

In the payments space, banks have partnered with technology platforms to manage the customer and product interface for both pre-paid and UPI-enabled payment solutions. In digital lending, banks, at the origination stage, are beginning to rely on credit-scoring procedures of non-bank partners that use non-conventional data to perform a credit risk analysis. The market is also likely to see post origination deals, such as securitisation of loan portfolios, risk sharing and back-end bank participation structures.

Payment companies have been pushing for inter-operability and a level playing field between banks and non-banks. In 2018, the Reserve Bank of India (“RBI”) issued guidelines for inter-operability of all mobile wallets (enabling wallet-to-wallet transfers across multiple issuers). Under the interoperability guidelines, issuers of pre-paid payment instruments have

the option of enabling inter-operable transactions between fully KYC-compliant pre-paid payment instruments by relying on United Payments Interface or card networks infrastructure. As the sector evolves, and regulation increases, the RBI is likely to be more comfortable giving non-bank players access to the payments, financial and digital infrastructure that banks are able to access.

While FinTech has taken rapid strides in India in the digital payments and lending space, the same is not true for cryptocurrency, where there has been considerable regulatory resistance. In April 2018, the RBI issued a circular prohibiting any bank or other entity licensed by the RBI from dealing in, settling or enabling any buying or selling of cryptocurrency with the intent to ring-fence such regulated entities from the risks associated with trading in virtual currencies, and also to protect against money-laundering risks generally associated with the use of cryptocurrency. While cryptocurrency is not legally prohibited, the RBI has on several occasions publicly stated that it does not view cryptocurrency as a valid payment system. The restrictions on cryptocurrency have prevented any significant growth in usage. There are, however, a few players in India, but given the regulatory constraints, peer-to-peer trading has emerged as one of the most common use cases. There has been some discussion on the Government of India formally banning the use and trading of cryptocurrency in India, but no draft or formal legislation has been introduced as of yet.

FinTech offering in India

The key FinTech products offered by financial services companies and other entities operating in the FinTech space in India are:

- **Pre-paid payment instruments:** Pre-paid payment instruments (“**PPIs**”) are instruments that facilitate the purchase of goods and services (including financial services, remittance facilities, etc.) against a “stored value” on such instruments. In India, PPIs may be issued by banks and eligible non-bank entities as pre-paid cards or virtual wallets. PPIs may be issued under one of three categories: (i) closed-system PPIs; (ii) semi-closed system PPIs; and (iii) open system PPIs.

A closed-system PPI is one that is issued by an entity to facilitate the purchase of goods and services from the issuer entity only and does not permit cash withdrawal. Semi-closed system PPIs may be used by customers for the purchase of goods and services from a group of identified merchants and service providers, who have at the back-end contracted with the issuer entity for accepting the PPI as a valid mode of payment. As with a closed PPI, a semi-closed PPI also cannot offer cash withdrawal. An open system PPI may only be issued by banks and may be used at any merchant location for the purchase of goods and services (including financial services and remittance facilities, etc.) and may also be used by customers for cash withdrawals.

- **UPI payments:** The Unified Payments Interface (“**UPI**”) is a payments platform managed and operated by the National Payments Corporation of India (“**NPCI**”). The UPI enables real-time, instantaneous, mobile-based bank-to-bank payments. The UPI primarily relies on mobile technologies and telecommunication infrastructure to offer easily accessible, low-cost and universal remittance facilities to users. UPI-enabled payments constitute a significant percentage of the consumer-to-merchant and peer-to-peer digital payment transactions.
- **Digital lenders:** With increasing advances in technology and telecommunications infrastructure, several non-banking financial companies (“**NBFCs**”) in India have

moved to digital platforms for credit products, particularly to SME and retail clients. These NBFCs have developed interactive applications and websites to enable end-to-end digital customer journeys – starting with onboarding and initial credit verification and checks, and then subsequently for execution of loan documents and disbursement.

- **Peer-to-peer lending platforms:** Peer-to-peer (“**P2P**”) lending platforms are online platforms which offer loan facilitation services between lenders registered on the platform and prospective borrowers. Under RBI regulations, P2P lending platforms may be operated by eligible Indian companies registered with the RBI as a non-banking financial company – P2P lending platform. P2P lending platforms act as intermediaries providing an online marketplace for P2P lending in a regulated environment.
- **Payment aggregators/intermediaries:** Payment aggregators or intermediaries are entities which facilitate online sale and purchase transactions primarily on e-commerce platforms. Such entities facilitate collection of electronic payments from customers for goods and services availed and the subsequent transfer of payments to merchants.
- **Payments banks:** Payments banks are entities licensed by the RBI to offer basic banking services digitally to their customers. Payments banks are permitted to accept small deposits (up to INR 100,000) from their customers. However, payments banks are not permitted to give loans, issue credit cards or offer any credit products. The regulatory intent behind payments bank licences was primarily to increase financial inclusion, especially in the low-income segments and to promote digital payments and digital banking services in the country.

Regulatory and insurance technology

Regulatory changes around e-KYC and Aadhaar

A key regulatory development that has had a significant impact on the FinTech ecosystem in India is the Indian Supreme Court’s judgment in *Justice (Retd.) K. Puttaswamy & Ors. v. Union of India* (“**Aadhaar Judgment**”) and consequent legislative changes. The Supreme Court’s decision in the Aadhaar Judgment restricted private bodies from undertaking Aadhaar e-KYC authentication (“**e-KYC**”) to verify the identity of their customers.

Following the Aadhaar Judgment, FinTech players faced significant challenges in onboarding new customers. Aadhaar-based e-KYC authentication facilities offered by the Unique Identification Authority of India (“**UIDAI**”) provided a convenient and easily accessible tool for FinTech players to verify the identity of new customers. The Supreme Court’s prohibition on access to the Central KYC Registry by private entities, in the absence of adequate legislative backing, made it operationally difficult for FinTech players to complete identity verification of their customers in a cost-effective manner. FinTech players in discussions with the UIDAI subsequently developed innovative ways to leverage the existing Aadhaar ecosystem (without accessing the Central KYC Registry) to complete identity verification of their customers, including use of QR code-based technologies, xml files, and masked Aadhaar files, which evolved primarily as market practice to ensure compliance with KYC regulations in a cost-effective manner, and which have now been recognised as legally valid methods of undertaking identity verification.

InsurTech

While InsurTech in India is currently in the early stages of growth, it has disrupted the traditional supply chain of insurance products in the country. Several players in the insurance

sector have partnered with technology partners and other FinTech players to offer a range of digital insurance products to their customers. For example, several payment wallets operating in the country have tied-up with insurance companies to offer insurance products to existing customers through their digital platforms. In addition to partnering with FinTech players like payments wallets, insurance providers have also set up independent digital platforms for offering insurance products to existing and new customers.

The key regulations governing InsurTech in India include the Guidelines on Insurance e-commerce dated March 9, 2017, the Guidelines on Insurance Repositories and electronic issuance of insurance policies dated May 29, 2015, the Issuance of e-insurance Policies Regulations, 2016, each issued by the Insurance Regulatory and Development Authority of India (“**IRDAI**”) to regulate and govern the provision of digital insurance products by eligible insurance providers to new and existing customers.

An important area of discussion in relation to the offering of insurance products in India is the bundling of insurance products with other goods and services (including financial products). The concerns around the packaging of insurance products with other products primarily include inadequate disclosure to the customer of the characteristics of the bundled insurance products, restrictions on consumer choice or the freedom to make informed choices or comparisons with other products available in the market, and undue influence over the customers by the provider of the packaged bundled products. With advances in technology and fast-paced developments in the FinTech market, opportunities to bundle insurance products with other financial products have become easier and convenient. In 2012, with a view to regulate bundling of insurance products with other goods and services, the IRDAI released a discussion paper on “tying and bundling insurance policies with other services and goods” and invited comments from the public. However, the discussion paper could not culminate into codified guidelines or regulations to regulate the bundling of insurance products.

Regulatory bodies

Reserve Bank of India

The primary regulator for FinTech in India is the central bank – the Reserve Bank of India. The RBI initially followed a light-touch approach to FinTech regulation, but more recently has moved closer towards a full-regulation model. Non-bank payment players, for example, now need to comply with customer onboarding and KYC procedures similar to those required of banks. With the absence of any consolidated regulation or policy guideline for FinTech, the regulatory landscape is decidedly fragmented, making it challenging to navigate. The RBI has generally been quick to respond to market changes and technological advances, and there have been several changes and updates in the law over the last few years to appropriately accommodate such developments.

Ombudsman Scheme for Digital Transactions

The RBI has mandated FinTech players to establish adequate mechanisms to address customer complaints in respect of products they offer. The RBI issued the Ombudsman Scheme for Digital Transactions on January 31, 2019, appointing RBI officers as ombudsmen to enable customers to report complaints against non-bank entities participating in a payment system on grounds including deficiency of service, unauthorised money transfers, and failure to initiate refunds. To ensure compliance, FinTech entities are required to appoint nodal officers responsible to represent them before the ombudsman and to abide by any award or directions issued by the ombudsman in relation to a customer complaint. The Ombudsman

Scheme for Digital Transactions is similar in ambit and scope to the Ombudsman Scheme for Non-Banking Financial Companies issued by the RBI on February 23, 2018.

In addition, with a view to protect users of mobile wallets and other digital payment tools, the RBI has issued multiple directions limiting liability of customers in case of unauthorised electronic payment transactions. The directions primarily prescribe the maximum financial exposure customers may be subject to in cases of fraud, negligence or other breaches in the digital payments ecosystem resulting in unauthorised payment transactions, causing loss to customers.

UIDAI

The UIDAI is the statutory body responsible for administering the Aadhaar programme – the largest identity project in India (and one of the largest identity projects globally). The UIDAI has been central to the rules and framework governing use of Aadhaar by FinTech players as a means for customer onboarding and verification.

Anti-money laundering

The primary anti-money laundering regulations governing entities offering financial products in India are the Prevention of Money Laundering Act, 2002 (“**PMLA**”), the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (“**PML Rules**”) and the RBI’s Master Directions on Know Your Customer dated February 25, 2016 (as amended from time to time) (“**KYC Master Directions**”). Under the KYC Master Directions, all entities regulated by the RBI must undertake identity verification of their customers before commencing any account-based relationship with such customers. Before the Aadhaar Judgment, regulated entities (including banks as well as non-bank entities) were permitted to utilise the e-KYC facility offered by the UIDAI to complete identity verification of their customers. E-KYC authentication involves access to the Central KYC Registry and retrieval of specified identification data to complete identity verification of individuals. In the Aadhaar Judgment, while addressing concerns around Aadhaar data privacy, the Supreme Court of India prohibited private bodies from accessing the Central KYC Registry for undertaking e-KYC on the basis of a private contract with customers, unless such access is backed by legislation. The Supreme Court also struck down sections of the PML Rules, which made the collection of Aadhaar by regulated entities mandatory before undertaking financial transactions with customers. Following the Aadhaar Judgment, and to ensure continuity of business on the basis of feedback received from market players, the UIDAI implemented new innovative methods to assist regulated entities in leveraging Aadhaar without accessing the Central KYC Registry (in compliance with the Aadhaar Judgment), to undertake identity verification of customers. These methods implemented by the UIDAI include masked Aadhaar, xml files and QR code-based verification processes that may be used by regulated entities for identity verification. The UIDAI has assumed significance as a regulator supplemental to the RBI, to the extent of using Aadhaar as a tool for KYC verification.

Key regulations and regulatory approaches

Key regulations governing FinTech in India

The regulatory landscape governing FinTech in India is largely fragmented, and there is no single set of regulations or guidelines which uniformly govern FinTech products in India. The absence of a consolidated set of regulations or guidelines governing FinTech products in India makes it difficult to navigate the regulatory landscape governing FinTech in India.

The regulatory framework primarily consists of:

- Payment and Settlement Systems Act, 2007: The Payment and Settlement Systems Act, 2007 (“**PSS Act**”) is the principal legislation governing payments regulation in India. The PSS Act prohibits the commencement and operation of a “payment system” without prior authorisation of the RBI. The PSS Act defines a “payment system” as “*a system that enables payment to be effected between a payer and a beneficiary, involving clearing, payment or settlement service of all of them, but does not include a stock exchange*”. Payment systems include the systems enabling credit card operations, debit card operations, smart card operations, money transfer operations, PPIs, etc.
- Master Direction on Issuance and Operation of Prepaid Payment Instruments: The Master Direction on Issuance and Operation of Prepaid Payment Instruments issued by the RBI on October 11, 2017 and amended from time to time (“**PPI Master Directions**”) prescribe the eligibility criteria for PPI issuers, permissible debits and credits from PPIs and other operational guidelines to be followed by PPI issuers while issuing PPIs to their customers in India. PPIs fall within the definition of a “payment system” under the PSS Act and are therefore required to comply with the PSS Act and the PPI Master Directions.
- NPCI Guidelines governing UPI Payments: UPI Payments in India are primarily governed by the UPI Procedural Guidelines and the UPI Operating and Settlement Guidelines issued by the NPCI. Under the current framework, only banks can integrate with the UPI platform to provide money transfer services to their customers. Banks are, however, permitted to engage technology providers for the design and operation of mobile applications for the purpose of UPI payments, subject to compliance with certain eligibility and prudential norms prescribed by the NPCI.
- NBFCs: NBFCs are primarily governed by the Reserve Bank of India Act, 1934 and a series of master directions and circulars regulating the licensing and operation of NBFCs in India. The RBI has set out certain thresholds to determine whether an entity will be classified as a financial services company requiring licensing. Most digital lenders operating in India are licensed as NBFCs. The key regulations governing NBFCs in India include Master Direction – NBFC – Systemically Important Non-Deposit taking Company and Deposit taking Company (Reserve Bank) Directions dated September 1, 2016 (as amended from time to time), Master Direction – NBFC – Non-Systemically Important Non-Deposit taking Company (Reserve Bank) Directions dated September 1, 2016 (as amended from time to time), and Master Direction – NBFC – Acceptance of Public Deposits (Reserve Bank) Directions dated August 25, 2016 (as amended from time to time).
- Guidelines regulating P2P lending platforms: P2P lending platforms are primarily governed by the Master Directions – NBFC – Peer to Peer Lending Platform Directions 2017, which prescribe lender exposure norms and aggregate borrowing limits in relation to operation of P2P lending platforms in the country.
- Guidelines governing payment aggregators/intermediaries: The circular on “*Directions for opening and operation of Accounts and settlement of payments for electronic payment transactions involving intermediaries*” dated November 24, 2009 (“**Payment Intermediary Circular**”) sets out the legal framework applicable to payment intermediaries operating in India. Payment intermediaries such as payment gateways, payment aggregators, etc. are required to comply with the operational guidelines prescribed under the Payment Intermediary Circular in the operation of intermediary systems in India.

- RBI Guidelines on Payments Banks: The Operating Guidelines for Payments Banks dated October 6, 2016 and Guidelines for Licensing of Payments Banks dated November 27, 2014 issued by the RBI are the primary regulations governing licensing and operation of payments banks in the country. These guidelines, *inter alia*, provide eligibility criteria for registration, permissible operations and other operational guidelines for payments banks operating in the country.
- Anti-money laundering regulations: The key regulations prescribing anti-money laundering norms and operational guidelines for entities engaged in providing financial services in the country to prevent money laundering are contained in the PMLA, the PML Rules and the KYC Master Directions.
- Data privacy and protection: Access to customer data, data privacy and protection have each become an increasingly important issue with FinTech platforms collecting and storing various forms of customer personal, financial, and behavioural data. India does not today have a comprehensive data privacy framework. The Information Technology Act 2000 and the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 are the two key regulations governing protection of personal data. The Justice Srikrishna Committee constituted by the Government of India to develop a data protection regulatory framework issued a set of recommendations and submitted the Personal Data Protection Bill in July 2018. The proposed Personal Data Protection Bill is currently under review and discussion by the Government.

Regulatory approaches

Data protection regulation

While regulations governing FinTech in India have not substantially been influenced by international or supranational regulatory regimes (for example, the Indian Government's continued resistance to recognition of cryptocurrency), one area where Indian regulations have relied on global precedent is data protection laws. The draft Personal Data Protection Bill is modelled along the lines of the General Data Protection Regulation ("GDPR") and adopts the key principles of the GDPR, including fair and reasonable processing, purpose limitation, collection limitation, and data storage limitation.

Regulatory sandboxes

The RBI has typically dealt with new development in the FinTech space by inviting comments from the general public, market players and other stakeholders before issuing regulations governing new innovative products in the FinTech space. The RBI recently released the "Draft Enabling Framework for Regulatory Sandbox" inviting comments from the public and concerned stakeholders on proposed guidelines governing regulatory sandboxes proposed to be set up by the RBI to test new products in a controlled regulatory environment under close supervision. Under the proposed regulatory sandbox framework, start-ups (defined as a company in business for no longer than seven years) which satisfy the eligibility criteria will be selected for testing their products in the regulatory sandbox. The eligibility criteria include parameters such as: (i) net worth of at least INR 5 million; (ii) satisfactory credit score; (iii) promoters and directors of the applicant entity meeting the prescribed "*fit and proper*" criteria; (iv) ability to comply with personal data protection laws; and (v) adequate IT infrastructure and safeguards to protect against unauthorised access, destruction and disclosure. The sandbox is intended to allow for testing of products and technology that: (i) are not currently governed by regulations and face some form of

regulatory barrier in implementation; (ii) require certain regulatory relaxations for testing; and (iii) seek to improve delivery of financial services. The RBI has indicated that the solution proposed for sandboxing must highlight an existing gap in the financial ecosystem and specifically address how this can be solved.

The RBI contemplates product testing by 10–12 FinTech start-ups in a single regulatory sandbox cohort (i.e. end-to-end sandbox process), where products broadly fall within a shared theme. There is a requirement for the test scenarios and expected outcomes to be clearly defined upfront. The entity must report results to the RBI on an ongoing basis, as per a pre-agreed schedule. While certain regulatory requirements may be relaxed for the duration of the sandbox, the RBI has made it clear that applicants will have to continue to comply with data protection laws and KYC requirements. And, separately, applicants will continue to be liable to customers for financial products tested in the sandbox. The framework outlines the five stages of the sandbox process for a single cohort, each of which shall be monitored by the FinTech Unit at the RBI (“**FTU**”): (i) Stage 1: preliminary screening of applications to the cohort (four weeks); (ii) Stage 2: finalisation of test design by the FTU via an interactive process with applicants (three weeks); (iii) Stage 3: application assessment and vetting of test design by the FTU (three weeks); (iv) Stage 4: testing by the FTU based on empirical evidence and data (12 weeks); and (v) Stage 5: evaluation by the FTU of the final outcome of the testing of the product or technology that was sandboxed (five weeks).

Similar to the regulatory sandbox proposed by the RBI for FinTech products, the IRDAI and the Securities and Exchange Board of India (“**SEBI**”) have proposed similar regulatory sandboxes products in the InsurTech space, and market-linked financial products offered by entities regulated by them, respectively.

The shift from “light touch” regulation to more “fully-fledged” regulation has increased the costs of operation for FinTech players, particularly in the payments space. The next significant regulatory development will be the adoption of the Personal Data Protection Bill. There are several industry bodies that have commenced the groundwork to sensitise FinTech players to the key aspects of compliance with this data legislation.

Restrictions

Pre-paid wallet issuers

Under the PPI Master Directions, in order to be eligible to obtain a certificate of authorisation from the RBI for issuing PPIs in India, entities must have a minimum positive net worth of INR 50 million; and by the end of the third financial year from the date of receiving final authorisation from the RBI, such entities must achieve a minimum positive net worth of INR 150 million.

NBFCs

Companies undertaking the business of a non-banking financial institution as their principal business are required to obtain a certificate of registration as an NBFC from the RBI. The RBI has further clarified that a company having financial assets which amount to more than 50% of its total assets (netted off by intangible assets), and income from financial assets amounting to more than 50% of the gross income, is considered to be engaged in the principal business of a non-banking financial institution (“**Asset Income Test**”). The Asset Income Test also requires a licensed NBFC to ensure that its principal business activities continue to be linked to provision of financial services. Most digital lending platforms in India operate as licensed NBFCs.

Payments banks

Payments banks operating in India must have a minimum paid-up equity capital of INR 1 billion and a leverage ratio of not less than 3%; i.e., the outside liabilities of a payments bank should not exceed 33.33 times its net worth. In addition, the RBI has clarified, in case the promoter entity of a payments bank intends to engage in other financial and non-financial activities, that such activities shall be kept distinctly ring-fenced and must not be co-mingled with the banking business of the payments bank.

Cross-border business

Developments in the FinTech space in India have also resulted in the emergence of several cross-border payment products in India. Under Indian law, foreign currency transactions are governed by the Foreign Exchange Management Act, 1999 and the rules and regulations made thereunder (“**FEMA**”). The directions issued by the RBI under the FEMA permit Authorised Dealer Category II; i.e., money changers to issue foreign currency pre-paid cards in India to Indian residents in accordance with the FEMA. Additionally, the PPI Master Directions permit eligible entities to issue PPIs for cross-border transactions. Authorised Dealer Category I Banks are permitted to issue semi-closed and open system PPIs for use in permissible current account transactions (including purchase of goods and services), provided that such PPIs are fully-KYC compliant, the transactions are in accordance with the FEMA, and are subject to a transaction limit of INR 10,000 per transaction and INR 50,000 per month.

Further, under the PPI Master Directions, permitted bank and non-bank PPI issuers (appointed as agents of an authorised overseas principal) may receive inward remittances under the money transfer service scheme, provided that such PPIs are fully KYC-compliant, reloadable, are issued in electronic form and the amounts of inward remittance do not exceed INR 50,000 per transaction.

**Shilpa Mankar Ahluwalia****Tel: +91 98 7100 4853 / Email: shilpa.mankar@AMSShardul.com**

Shilpa Mankar Ahluwalia leads the FinTech practice at Shardul Amarchand Mangaldas & Co (“the Firm”) and has worked in the banking & finance and financial services M&A practice groups. She has advised several payment solution platforms in connection with their products in India, including Vodafone, Golbibo, Airtel, Paypal, Facebook, American Express, Kitecash, and Zeta. Shilpa has also advised various companies, banks and financial institutions in connection with their financing activities (issue of bonds and non-convertible debentures, plain vanilla and structured financings, loan syndication and guarantee structures). Her clients include the International Finance Corporation, American Express, Nokia Corporation, Eton Park, FIMBank, Farallon Capital, Bank of America Merrill Lynch, and Bank of Tokyo Mitsubishi. She has also advised on specialised financial products such as factoring and mortgage guarantees (including the first mortgage guarantee deal in India). She was on the Government drafting committee for the Factoring Act and has supported MFIN in their policy initiative with the RBI. She holds an LL.M. from the Columbia University School of Law, New York, and a B.A. LL.B. (Hons.), from the National Law School of India University, Bangalore. Prior to joining the Firm, Ms. Ahluwalia worked with Davis Polk & Wardwell, New York.

**Himanshu Malhotra****Tel: +91 92 0598 4244 / Email: himanshu.malhotra@AMSShardul.com**

Himanshu Malhotra is a member of the FinTech practice group at the Firm and has worked in the banking & finance practice group. He has advised several digital payment platforms, payment wallets and other FinTech players operating in the country in designing and structuring their financial products. He holds a B.A. LL.B (Hons.), from NALSAR University of Law, Hyderabad.

Shardul Amarchand Mangaldas & Co

Amarchand Towers, 216 Okhla Industrial Estate, Phase III, New Delhi – 110 020, India
Tel: +91 11 4159 0700 / +91 11 4060 6060 / URL: www.amsshardul.com

Indonesia

Harun Reksodiputro & Dion Alfadya
Ginting & Reksodiputro in association with Allen & Overy LLP

Approaches and developments

The fintech-related regulations in Indonesia have been in place since the issuance of Bank Indonesia (**BI**) Regulation on card-based payment instruments in December 2004. This was followed by the issuance of the fund transfer regulation in December 2006 and the electronic money (e-money) regulation in April 2009; however, there seemed to be few developments in this area of law compared to the development of the fintech business models seen in other jurisdictions. The regulatory bodies overseeing fintech sectors (i.e. BI and the Indonesian Financial Service Authority, *Otoritas Jasa Keuangan*, **OJK**) did not seem to be able to catch up with the varying fintech business models, perhaps primarily because the business players themselves were not as aggressive in entering into this business sector. There were times when BI ceased issuing fintech-related licences (e.g. e-money licences). This was presumably because it was quite nervous knowing that the e-money business could involve a significant amount of the public's money (and therefore could put the public's money at risk), but the underlying regulations did not seem to contain sufficient details to address that risk.

The significant developments in the fintech-related regulations began in 2016 with the issuance of regulations on: (i) payment processing services in November 2016; (ii) peer-to-peer (**P2P**) lending in December 2016; (iii) the national payment gateway in June 2017; (iv) fintech operation in November 2017; (v) fintech innovation in financial services in August 2018; and (vi) equity crowd funding in December 2018. These significant developments could be mainly attributed to the rising popularity of e-retail and online marketplace providers (including those providing ride-hailing and other on-demand services such as food delivery and shopping) and the exponential deepening of market penetration enabled by affordable mobile devices and internet connection. Another driving aspect could also be the surge of the P2P business players from China entering into Indonesia.

The most significant impact from the issuance of the foregoing fintech regulations is the approach taken by each BI and OJK in determining whether a specific fintech activity is subject to any licensing requirements. Previously, BI and OJK would strictly limit their authority to regulate activities that qualify or correspond with the specific elements set out in the regulations. Consequently, market participants would usually conduct a study to check if their proposed offerings would qualify as those specific elements set out in the regulations. With the new approach, specifically through the implementation of the mandatory fintech registration and sandbox mechanism, BI and OJK could take a more flexible approach in determining their authority over the market participants. It remains to be seen how the implementation of the regulatory sandbox will turn out, given the significant number of

fintech players (and business variations) out there and taking into account the limited resources that the relevant authorities have.

In the mandatory fintech registration, both BI and OJK set a broadly defined criteria of fintech services (e.g. innovative in nature, may have an impact on the existing products, services, technologies and/or financial business models, and can be widely used), and require any provider whose services meet the criteria to register itself with the regulatory bodies. Following the registration, BI or OJK may impose a licensing requirement on certain service providers as it deems necessary. In effect, BI or OJK can now monitor and regulate any fintech services that were previously not explicitly captured by the regulations.

Further, in the last three years, OK and BI as the respective authorities overseeing the financial institutions and payment system, have also given more attention to the fintech sector due to the rapid growth in market penetration as well as the M&A activities in the fintech industry led by the national and multinational online marketplaces, e-retail providers and other tech start-ups, including by limiting the foreign ownership in certain fintech lines of business.

Fintech offering in Indonesia

Electronic money (e-money)

The use of e-money has increased rapidly in recent years. As well as being used as one of the means of payment for e-retail and marketplace providers in the gaming, consumer goods, ride-hailing, healthcare and logistics industries, e-money is also widely used in other brick-and-mortar retail businesses. The Indonesian government has also in many instances expressed its support for non-cash payment, making the use of e-money more attractive. One of the moves initiated by the government was the implementation of non-cash payment exclusively on all toll roads across Indonesia since 2017. Some Indonesian state-owned enterprises (notably banks) have their own e-money products so as to ensure they do not miss the bandwagon.

The most recent regulation on e-money operation is BI Regulation No. 20/6/PBI/2018 dated 3 May 2018 on E-Money (**BI E-Money Regulation**). The BI E-Money Regulation defines e-money as a payment instrument in which:

- (a) it is issued based on the value of money paid in advance to the issuer;
- (b) the value of money is stored electronically in a server or on a chip; and
- (c) the value is managed by the issuer, and does not constitute savings under the prevailing banking laws and regulations.

BI is the main regulatory authority of the e-money business and has the authority to: (i) issue an e-money business licence; (ii) supervise the e-money business operation; and (iii) impose administrative sanctions for any violation of, and/or non-compliance with, the BI E-Money Regulation.

The BI E-Money Regulation classifies e-money service providers into six categories:

- (a) **E-Money Issuer** – refers to a party that issues the e-money.
- (b) **E-Money Acquirer** – refers to a party that enters into a cooperation agreement with goods and/or services merchants so that the merchants are able to process data relating to e-money issued by another party. The E-Money Acquirer is also responsible for the settlement of payments to the merchants.
- (c) **E-Money Principal** – refers to a party responsible for: (i) channelling the e-money

transaction data through a network; (ii) the implementation of the rights and liabilities calculation; (iii) the payment settlements; and (iv) the stipulation of business mechanics and procedures.

- (d) **E-Money Switching Operator** – refers to a party that procures and operates the infrastructure used as the centre and/or hub for the channelling of payment transactions data using e-money.
- (e) **E-Money Clearing Operator** – refers to a party that calculates the financial rights and liabilities of each E-Money Issuer and/or E-Money Acquirer in the context of e-money transactions.
- (f) **E-Money Final Settlement Operator** – refers to a party that acts and is responsible for the final settlements of the financial rights and liabilities of each E-Money Issuer and/or E-Money Acquirer in the context of e-money transactions based on the calculations made by an E-Money Clearing Operator.

The E-Money Issuers and E-Money Acquirers are considered front-end providers, while the rest are back-end providers. An e-money service provider can only provide services at either the front-end or the back-end. For example, an E-Money Issuer can also be an E-Money Acquirer, but cannot be an E-Money Principal. The rationale for this grouping is to avoid potential conflicts of interest in operating front-end as well as back-end services. Aside from the front-end and back-end classification, the BI E-Money Regulation also recognises closed-loop services and open-loop services. Closed-loop e-money is defined as e-money that can only be used as a payment instrument for goods/services of the E-Money Issuer. Meanwhile, open-loop e-money is defined as e-money that can be used as a payment instrument for goods/services of other parties aside from the E-Money Issuer.

Payment processing services

Various payment processing services hold a substantial role in both the conventional offline and the newly emerging e-retail sectors, especially in bridging the online-to-offline transactions and reducing “friction” in the payment process.

BI is the main regulatory authority of the payment transaction processing business pursuant to BI Regulation No. 18/40/PBI/2016 dated 8 November 2016 on Payment Transaction Processing Activities (**BI Payment Processing Regulation**). The BI Payment Processing Regulation classifies payment service processors into 10 categories (each a **Payment Processor**):

- (a) **Principal** – refers to a party responsible for: (i) channelling electronic transaction data through a network; (ii) the implementation of the rights and liabilities calculation; (iii) the payment settlements; and (iv) the stipulation of business mechanics and procedures.
- (b) **Switching Operator** – refers to a party that procures and operates the infrastructure used as the centre and/or hub for the channelling of the data relating to payment transactions using cards, e-money and/or fund transfer.
- (c) **Issuer** – refers to a party that issues e-money, credit cards or debit cards.
- (d) **Acquirer** – refers to a party that enters into a cooperation agreement with goods and/or services merchants so that the merchants are able to process data relating to electronic payment instruments issued by another party. The Acquirer is also responsible for the settlement of payments to the merchants.
- (e) **Payment Gateway Operator** – refers to any party that enables merchants to process

payments of transactions that use electronic payment instruments such as cards, electronic money and/or proprietary channels.

- (f) **Payment Clearing Provider** – refers to a party that calculates the financial rights and liabilities of each Issuer and/or Acquirer in the context of electronic payment transactions.
- (g) **Final Settlement Operator** – refers to a party that acts and is responsible for the final settlements of the financial rights and liabilities of each Issuer and/or Acquirer in the context of electronic payment transactions based on the calculations made by a Clearing Operator.
- (h) **Fund Transfer Provider** – refers to any party that holds a licence from BI to provide fund transfer services.
- (i) **E-Wallet Operator** – refers to any party that holds a licence from BI to provide e-wallet services.
- (j) **Other Payment Processors** as stipulated by BI – refers to parties that provide payment processing services at the stage of authorisation, clearing and/or final settlement activities other than the Payment Processors mentioned in paragraphs (a) to (i) above.

Fund transfer

A fund transfer service, a relatively traditional service, has discovered vast, new market development opportunities in the wake of both the e-retail and marketplace industries. Most established marketplace and e-retail providers include fund transfer capability as part of its overall services to its customers.

The current regulation on fund transfer is BI Regulation No. 14/23/PBI/2012 on Fund Transfer (the **BI Fund Transfer Regulation**). The BI Fund Transfer Regulation defines a fund transfer as a series of activities that begins with an instruction from an originator, with the purpose of transferring a certain fund to the beneficiary as stated in the instruction, and ends when the fund is received by the beneficiary. The BI Fund Transfer Regulation also classifies the fund transfer processors into the following:

- (a) **Originator** – a party that first issues the fund transfer instruction.
- (b) **Sender** – the Originator, Originator Processor and all Intermediate Processor(s) that issue the fund transfer instruction.
- (c) **Receiving Processors** – the Originator Processor, Intermediate Processor, and Final Processor which receive the fund transfer instruction.
- (d) **Originator Processor** – a processor that receives the fund transfer instruction from the Originator to pay or instruct another fund transfer processor to pay a certain amount of funds to the beneficiary.
- (e) **Intermediate Processor** – a processor that is not an Originator Processor or a Final Processor.
- (f) **Final Processor** – a processor that transfers or delivers the funds to the beneficiary.

Capital raising (P2P lending and equity crowd funding)

OJK has only recently regulated two forms of tech-enabled capital raising in Indonesia: (i) PSP on 29 December 2016 through the promulgation of OJK Regulation No. 77/POJK.01/2016 (**P2P Regulation**), and (ii) equity crowd funding on 31 December 2018 through the promulgation of OJK Regulation No. 37/POJK.04/2018 (**Crowd Funding Regulation**).

Despite the recent breakthrough of recognising and regulating these two forms of capital raising, OJK has taken a cautious approach with these industries. For example: (i) OJK has set lending and crowd funding limitations to confine these industries to catering to small-to-medium enterprises, and (ii) OJK has only handed out P2P licences to a handful of companies,¹ and to our knowledge has yet to issue an equity crowd funding licence. This cautious approach is likely to be in part designed to limit the disruption to existing, traditional fund-raising institutions such as banks, financing companies, and the capital markets – all industries under the authority of OJK.

Of the two (P2P and equity crowd funding), P2P has grown more in recent years, in part because it has been regulated for longer and, prior to the promulgation of the P2P Regulation, there have already been players in the P2P lending space using various structures to operate in Indonesia. For example, in a typical structure, foreign P2P lending platforms would lend to Indonesian-based lending cooperatives, which will in turn loan onwards to the debtors. Other online lending companies simply lent directly to the debtors, without a licence and was often accused of being illegal loan sharks. Media scrutiny of the practices of these supposed “online loan sharks” in part prompted the issuance of the P2P Regulation and OJK’s increased scrutiny to protect both the public and existing industry players. Other than issuing the P2P Regulation, OJK also regularly publishes a list of illegal online lending companies about which to warn the public to steer clear from them.

Key provisions of the P2P Regulation include: (i) a two-step licensing regime in which P2P lending platforms first register with OJK, following which it applies for a P2P licence; (ii) an 85% foreign ownership (direct or indirectly) cap; (iii) a maximum IDR2 billion per borrower lending limit; and (iv) prohibition for the P2P lending platform to borrow money (certain exemptions based on unwritten policies applied inconsistently). While some industry players may view P2P Regulation as restrictive, it is at least a first step in recognising the legality of P2P lending platforms.

While P2P is still in its infancy, equity crowd funding in Indonesia is yet to really kick off. Prior to the Crowd Funding Regulation, the existing regulations rule out a legal and viable equity crowd funding structure. Company and capital markets regulations effectively obliges companies that are crowdfunded to go through the public offering and are hence subject to various requirements of disclosure, obtaining OJK approval, and other various requirements applicable to a public offering which effectively made crowd funding untenable (especially for small-to-medium enterprises). These barriers have in the past led to platforms initially contemplating an equity crowd funding scheme to pivot to a P2P lending structure.

The Crowd Funding Regulation, however, effectively sets aside the abovementioned requirements to allow a crowd funding structure outside of the traditional capital markets. Key provisions of the Crowd Funding Regulation include: (i) an exception to the requirement for a public offering if the offering amongst others has obtained OJK approval; (ii) a limit of 300 shareholders and a maximum paid up capital of IDR30 billion in order not to qualify as a public company; (iii) a maximum IDR10 billion fundraising limit every 12 months for each issuer; (iv) a maximum limit of IDR10 billion of assets (outside of land and building) for the issuer; (v) a licensing requirement for the crowd funding platforms; and (vi) various requirements for the crowd funding platform to review, supervise and disclose information on the issuer; (vii) obligation for the crowd funding platform to provide an internal dispute resolution service mechanism; and (viii) restriction to have affiliated relationships between the crowd funding platform and the issuer. There are other various technical rules and restrictions – which is arguably more onerous than the P2P Regulations, and it remains to

be seen how these rules and restrictions will be implemented and whether the Crowd Funding Regulation is attractive enough to promote the growth of equity crowd funding.

Although there is optimism with OJK's approach of regulating P2P and equity crowd funding, it remains to be seen whether OJK will eventually relax the regulations to allow these sectors to further develop. OJK is also yet to regulate in depth other variation loan and equity structures including if a P2P company is actually giving on balance sheet loans through its holding company, instead of actually gathering funds from the public to be extended as loans (which is the main essence of a P2P lending business); and, as of now, "plain vanilla" structures are still predominant. Given the impression that OJK's primary focus is still on regulating the traditional industries (i.e. banks, multi finance, insurance and capital markets), OJK is likely to approach P2P and equity crowd funding with caution – as P2P and equity crowd funding can potentially disrupt the traditional industries OJK was primarily tasked to regulate and protect.

Regulatory and insurance technology

In Indonesia, regtech-related or insurtech-related regulatory development is not as advanced as the other fintech cohort. One of the possible reasons for this is that the tech-based services that could be generally seen as "regulatory or insurance technology", for example: KYC-related; electronic signature; and data processing services, can be captured by the existing regulations concerning conventional financial institutions, electronic information and transactions (albeit not seamlessly).

In terms of insurtech activities, we have seen in practice established insurance companies cooperating with tech-based companies which engage in data collection and analysis, cloud computing, KYC-related services and insurance policies marketplace. There are also a handful of tech-based on-demand healthcare service companies that cooperate with hospitals as third-party administrators of insurance claims.

Regulatory bodies

Supervision of the financial sector and system

There are two primary institutions in Indonesia which regulate the financial sector and system – BI and OJK. OJK is responsible for the regulation and supervision of all financial services which includes the traditional financial industries such as banks, capital markets, insurance, pension funds, and multi-financing, as well as newer industries such as peer-to-peer lending and equity crowd funding. BI, on the other hand, sets and regulates monetary policy and payment systems, with the latter encompassing e-money, payment processing and fund transfers.

Consumer protection

Although Indonesia has a National Consumer Protection Body, we have not seen it having a substantial role in protecting consumers in the financial services industry. The main regulators involved in consumer protection in the fintech space are OJK and BI, respectively, regulating the areas as previously mentioned above. OJK in particular has been proactive in trying to protect consumers, such as by regularly publishing a list of unlicensed P2P companies and a list of companies known to offer fraudulent investments. BI also has a consumer protection function which, amongst others, allows consumers to report complaints in relation to payment systems. As OJK and BI are the regulating authorities of financial services and payment systems respectively, players in those industries are likely to take heed of any consumer protection issues OJK and BI may raise.

Ministry of Communications and Informatics

The Ministry of Communications and Informatics (**MOC**) also plays a role in fintech, as electronic systems that have a public interest element must be registered with the MOC. This has been interpreted to include fintech-related applications and electronic systems. The MOC also regulates technical matters such as server location and also consumer data protection – which are both issues closely related to fintech.

Key regulations and regulatory approaches

Key regulations with respect to fintech activities include:

- (a) the BI E-Money Regulation;
- (b) the BI Payment Processing Regulation;
- (c) the BI Fund Transfer Regulation;
- (d) the P2P Regulation;
- (e) the Crowd Funding Regulation;
- (f) BI Regulation No. 19/12/PBI/2017 on Provision of Financial Technology;
- (g) OJK Regulation No. 13/POJK.02/2018 on Digital Fintech Innovation; and
- (h) BI Regulation No. 19/8/PBI/2017 on National Payment Gateway.

In light of these key regulations and as mentioned in the “Approaches and development” section above, we can see that there has been a shift in perspective by the relevant authorities in regulating certain fintech activities. Further, responding to the vast growth of e-money development, in May 2018 BI imposed more robust risk management and security standards through the issuance of the BI E-Money Regulation, requiring closed-looped e-money players meeting certain managed fund thresholds to obtain a licence (previously the licence requirement applied only to open-loop e-money), and imposing a foreign investment restriction on e-money licence holders at a maximum of 49% (direct and indirectly). OJK, in contrast, implemented a more lenient regulation in December 2018 for the conventional multi-finance sectors, i.e. the multi-finance companies that are now permitted to disburse cash directly to their debtors with certain limitations. This leniency could be seen as a measure by OJK to ensure that conventional multi-finance companies can compete against P2P lending companies. We do not believe that this shift in perspective is linear, but rather simply driven by the characteristics of the market and business models (perhaps also by the needs of the disrupted business players under the auspices of BI or OJK).

Restrictions

In addition to the various restrictions and limitations to the P2P lending and equity crowd funding as set out above, all fintech companies in Indonesia are prohibited from using any virtual currency as an instrument of payment in all of their activities.

Cross-border business

While there are no supra-national regulatory regimes or regulatory bodies that directly regulate fintech activities in Indonesia, both OJK and BI have cross-border collaborations with foreign financial authorities. OJK, for example, has entered into cooperation agreements or MOUs with regulators from Singapore, Australia, Japan, China and South Korea. In addition to an exchange of information in innovative financial services, some of the cooperation agreements, such as the cooperation agreement with Singapore, aims at

creating a framework to help fintech companies from each respective country to understand the rules and opportunities of the other country. BI, on the other hand, also has various collaborations with foreign regulators and is a part of various international institutions where there is sharing of information in the field of payment systems.

Yet aside from the formal collaborations outlined above, both OJK and BI are cognisant of how foreign regulators in various jurisdictions approach new disruptive developments in fintech. Both OJK and BI have adopted concepts such as the regulatory sandbox, and as a general approach, look at how other jurisdictions regulate a certain matter when contemplating whether to enact a regulation.

* * *

Endnote

1. Based on OJK's publication as per 31 May 2019, there are 106 P2P lending platforms registered and seven P2P lending platforms with a licence.



Harun Reksodiputro

Tel: +62 21 2995 1711 / Email: harun.reksodiputro@allenoverly.com

Harun specialises in corporate and commercial law, including share and asset acquisitions, joint ventures, corporate restructurings and dispositions, investments and divestments. He represents local and foreign companies, and has led successful negotiations on share purchase agreements, asset purchase agreements, joint venture agreements, and commercial agreements. He focuses on investors doing business in Indonesia through direct investment or the capital markets.

Harun continues to impress clients with his broad corporate knowledge, spanning M&A, investments and corporate restructuring, and he is acknowledged by sources as “a technically very good practitioner” (*Chambers Asia Pacific 2017 – Corporate/M&A – Indonesia*). Sources say Harun “knows the sector” (*The Legal 500 2017 – IT and telecoms – Indonesia*) and he is appreciated by clients for being “always reachable” (*Chambers Asia Pacific 2016*). Sources highlight that Harun is “attentive and experienced” and “a great asset to the firm” (*IFLR1000 2016*).



Dion Alfadya

Tel: +62 21 2995 1762 / Email: dion.alfadya@allenoverly.com

Dion is a experienced corporate and M&A lawyer in Ginting and Reksodiputro. His experience includes advising general corporate/commercial matters, which encompass joint ventures, foreign investment, contract-related issues, mergers & acquisitions and business restructurings. The notable industries that Dion is specialised in are IT/communication, pharmaceuticals, FMCG, and real estate.



Riandi Apriliansyah

Tel +62 21 2995 1724 / Email: riandi.apriliansyah@allenoverly.com

Riandi focuses on corporate financing & restructuring, acquisition financing, and M&A, particularly in the energy, retail and telecommunication sectors. He has also been involved in projects development (power, infrastructures and capital market transactions).

Ginting & Reksodiputro in association with Allen & Overy LLP

The Energy Building, 15th Floor Sudirman Central Business District Jl Jend Sudirman Kav 52-53, RT.5/RW.3, Senayan, Kebayoran Baru, Jakarta, 12190, Indonesia

Tel: +62 21 2995 1700 / URL: www.allenoverly.com/locations/asia-pacific/indonesia

Ireland

Liam Flynn & Lorna Daly
Matheson

Approaches and developments

Ireland is a leading European domicile for established and start-up FinTech businesses. This is unsurprising, given Ireland's traditional strengths in the internationally traded technology and financial services industries. According to the Ireland FinTech Census 2018 (Enterprise Ireland/Deloitte), 71% of Irish FinTech respondents do not require to be regulated by the Central Bank of Ireland ("Central Bank") due to their subsector, while 29% are currently regulated by the Central Bank or another EU regulator. The leading FinTech subsectors represented in Ireland are the RegTech and digital identity and payments/remittances spaces, with 17.5% and 12.7% shares respectively. Thirty-two per cent of Irish FinTechs reported anticipated global revenue growth of between 100–500%.

The Government of Ireland is strongly supportive of FinTech, recognising the significant benefits it can bring to consumers, economic growth, productivity and the competitiveness of the Irish economy. The Government, in its Strategy for the International Financial Services Sector ("IFS 2020"), has stated its commitment to developing Ireland as a global leader in the financial services sector, creating an environment in which both indigenous and multinational firms can draw on key governmental incentives and supports to grow their businesses. It is estimated that approximately 7,000 people are currently employed in the FinTech industry in Ireland, along with almost 40,000 in the wider financial services sector and over 100,000 in the technology sector.

The key elements of the Irish FinTech ecosystem are:

Industry organisations: the FinTech and Payments Association of Ireland, the Banking and Payments Federation of Ireland, FinTech Ireland and Financial Services Ireland.

State agencies: the Industrial Development Authority ("IDA"), Enterprise Ireland, and Ireland Strategic Investment Fund ("ISIF").

Incubators and accelerators: Dogpatch Labs, the Digital Hub, and start-lab/accelerators supported by organisations such as Bank of Ireland, Citi and MasterCard.

Successful FinTech enterprises: CurrencyFair, Swrve, TransferMate, and Fenergo, among others.

Sophisticated professional advisors: Lawyers, accountants, and technology consultancies.

Ireland's stable 12.5% rate of corporation tax on trading profits is an important element of its competitive offering to international business. Ireland also has tax legislation designed to make it attractive for holding companies and as regional headquarters, as well as other key tax benefits such as R&D credits. In addition to the potential for state funding/investment via the IDA, Enterprise Ireland and ISIF, the private funding sector is vibrant, though Ireland has seen relatively little crowdfunding or ICO activity.

Ireland's talent pool is a key attraction for FinTech operations. Dublin is a dynamic and open city that provides a welcoming home to globally mobile professionals. Hosting major European operations for top-tier technology companies such as Google, Facebook and Microsoft, Ireland has a rich and deep tech worker base. It retains close ties to and attracts high levels of FDI from both the UK and the US, the world's two leading FinTech start-up environments. With Brexit on the horizon, and the migration of significant financial services operations to Ireland in its wake, Ireland is an obvious choice for FinTech operations seeking a new but still familiar home in Europe.

Fintech offering in Ireland

Accelerator programmes are expanding their activities in Ireland, with Dublin being added as one of two accelerator locations by the NadiFin FinTech accelerator programme, and NDRC expanding its activities outside Dublin to Waterford and Galway. Dublin remains the hub for FinTech activities in Ireland, but other centres are seeing growth.

Ireland has won an outsized share of investment in corporate innovation labs, including Citi, MasterCard, Aon, Fidelity and First Data. In AI and RegTech, Enterprise Ireland and IDA have supported CeADAR, IC4 and GR3C, Ireland's research centres for AI, cloud computing and commerce and governance risk/compliance.

As Brexit looms, many payments and e-money firms that previously provided services across the EU on foot of a UK payments or e-money licence have sought to obtain Central Bank licences in Ireland so as to ensure continuity of operations. This has led to a very significant increase in the number of licensed payments and e-money firms, to 14 and eight respectively, and there are multiple further licence applications in the pipeline.

Despite the burgeoning start-up scene, the adoption of FinTech by mainstream financial services operators in Ireland and by consumers continues to lag behind. Digital challenger banks have not penetrated the Irish market to any significant extent and there are no "home-grown" challenger banks. European operators such as N26 and Revolut have "passported" their services into Ireland but have not yet posed an existential threat to traditional Irish banking houses. Robo-advice has yet to make an appearance in the mainstream investments market. Many life and health insurers are investigating the potential incorporation of wearable devices into insurance underwriting, and some of the main motor insurers, such as AIG and AXA, have launched safe driving apps that provide telematics-based discounts for drivers.

Regulatory and insurance technology

Like other advanced economies, Irish insurers are actively monitoring the "internet of things" and the development of AI and the resulting potential for more sophisticated underwriting approaches. As in other EU jurisdictions, GDPR compliance is the key legal concern here. The Central Bank has not yet revised or reviewed its conduct of business rules for insurers and intermediaries to address concerns that could arise from widespread adoption of InsurTech. The market potential for increased adoption of InsurTech is clear – witness La Parisienne's deal in 2018 to underwrite through Zego "on/off" insurance for Deliveroo drivers and others in the "gig" economy – but the regulatory regime has yet to catch up.

As regards RegTech, a survey published by RegTech Analyst in November 2018 showed seven Irish firms in the top 100 globally, ranking Ireland above Hong Kong and Singapore as a RegTech hub. Irish RegTech firms that have achieved international success include

AQMetrics and Gecko Governance. The Irish financial services industry is well aware of the potential to better deploy technology to achieve more efficient and cheaper compliance solutions, but as of yet the Central Bank has not taken explicit measures within the regulatory framework to incentivise the deployment of RegTech by Irish regulated firms.

Regulatory bodies

There is no dedicated Fintech regulator in Ireland. There is only one financial services regulator in Ireland, the Central Bank of Ireland, which is responsible for authorising and supervising providers of regulated financial services. The Central Bank is responsible for both prudential supervision and consumer protection of regulated entities which it has authorised. Where a regulated firm has been authorised by a supervisory authority in another jurisdiction, the home state regulator will be responsible for prudential supervision, but the Central Bank will be responsible for conduct of business supervision. The Single Supervisory Mechanism at the European Central Bank also directly supervises significant credit institutions and has exclusive competence for the authorisation of credit institutions (other than branches of third-country credit institutions).

Key regulations and regulatory approaches

Whether or not a Fintech business needs to hold a financial services authorisation will depend on the nature of the activities that the firm engages in. The majority of relevant regulated activities stem from EU directives, and each of the regimes below provide for a passporting regime which permits a provider authorised in one Member State to provide its services in other Member States, subject to notification requirements to the home and host state competent authorities.

Directive (EU) 2015/2366 (“PSD II”) was transposed into Irish law by the European Union (Payment Services) Regulations 2018 and regulates the provision of payment services. Fintech businesses engaged in regulated payment services (such as money remittance or operating payment accounts) are required to be authorised under PSD II. PSD II also introduced two new types of payment service: account information services; and payment initiation services.

Directive 2009/110/EC (“EMD”) was transposed into Irish law by the European Communities (Electronic Money) Regulations 2011, which regulate the issue and redemption of “electronic money”.

Directive 2014/65/EU (“MiFID II”) was transposed into Irish law by the (European Union (Markets in Financial Instruments) Regulations 2017) (the “Irish MiFID II Regulations”) and aims to create a single market for investment services and activities and to ensure a high degree of harmonised protection for investors in “financial instruments” in the EU. In the case of digital assets (whether in the form of tokens, coins or otherwise), where the coin, token or other asset qualifies as a “transferable security” or other “financial instrument”, the process by which the digital asset is created, distributed or traded is likely to involve some MiFID II investment services such as placing, dealing in or advising on “financial instruments”, requiring authorisation from the Central Bank (or the supervisory authority of another Member State of the EU). The operation of a trading platform for “transferable securities” and other “financial instruments” is a regulated investment service that requires authorisation under the Irish MiFID II Regulations. Accordingly, if the digital assets to be traded comprise “transferable securities” or other “financial instruments”, a MiFID II authorisation will be required. If the digital assets to be traded are not “transferable

securities” or other “financial instruments”, as is likely the case with pure utility tokens and payment tokens based on current law and practice, no MiFID II authorisation will be required. Prospectus regulation, deriving from EU law, may also be relevant where the digital asset constitutes a financial instrument and is either offered to the public in a Member State or is listed on a regulated market.

Directive 2011/61/EU (“AIFMD”) was transposed into Irish law by the European Union Alternative Investment Fund Managers Regulations 2013 (the “Irish AIFMD Regulations”) and lays down the rules for the authorisation, ongoing operation and transparency of the managers of alternative investment funds (“AIFMs”) which manage and/or market alternative investment funds (“AIFs”) in the EU. An “AIF” is defined in the Irish AIFMD Regulations as a collective investment undertaking, including investment compartments thereof, which raises capital from a number of investors with a view to investing it in accordance with a defined investment policy for the benefit of those investors (other than a collective investment undertaking that requires authorisation under the UCITS Directive (Directive 2009/65/EC)).

An AIFM covered by the parameters of the Irish AIFMD Regulations is not permitted to manage or market relevant AIFs unless authorised to do so by the Central Bank (or the supervisory authority of another Member State of the EU). Depending on how it is structured, an offering of digital assets could qualify as an AIF, to the extent used to raise capital from a number of investors with a view to investing the capital raised in accordance with a defined investment policy for the benefit of those investors. Firms involved in ICOs may therefore need to comply with AIFMD rules.

In addition to sector-specific requirements, Fintech businesses may need to comply with consumer protection legislation (depending on the nature of the customers), Central Bank conduct rules, anti-money laundering requirements and data protection legislation.

There are some financial services that Fintech firms can touch on, which are subject to domestic Irish legislation, including acting as a money transmission business, retail credit firm or credit servicing firm, all governed by Part V of the Central Bank Act 1997. Licences obtained under these regimes will not be available for passporting into other EU Member States, since the regulatory regimes in question do not derive from EU directives.

Although the Irish Department of Finance has consulted on this point, Ireland does not currently have a bespoke domestic regime for the regulation of crowdfunding. On 8 March 2018 the EU Commission published a proposal for a Regulation on European Crowdfunding Service Providers for Business, which includes a comprehensive authorisation and passporting regime for in-scope crowdfunding platforms across Europe. Once enacted at EU level, this will become directly effective under Irish law. Similarly, at present, Ireland does not have a bespoke regulatory regime for cryptocurrencies.

Restrictions

The main restriction on Fintech businesses seeking to operate in Ireland would be the requirement for authorisation if the proposed activities fall within the scope of one of the regulatory regimes listed above.

On 20 April 2018, the Central Bank launched its Innovation Hub. This is a direct and dedicated point of contact for firms developing or implementing innovations in financial services based on new technologies. This was to accommodate greater interaction with the growing number of Fintech businesses looking to set up operations in Dublin, or expand

their existing operations both in the regulated and unregulated space. A number of initiatives have been undertaken by different financial institutions applying distributed ledger technology, AI and robotics, and the Central Bank is keen to engage with innovators who are operating as regulated and unregulated entities in the financial services space.

The Central Bank has, like the European Supervisory Authorities, published warnings to consumers in relation to the unregulated nature of digital assets and other Fintech products.

Cross-border business

Ireland continues to develop as a Fintech hub and invest in attracting Fintech business to establish operations here. We have seen a number of cross-border firms enter the Irish market, particularly in the payments and e-money space. The Central Bank, as a national competent authority for Ireland, also participates in discussions at European level and through those into discussions at international level (e.g. the Basel Committee agenda regarding cryptocurrencies) in relation to supervisory approaches to Fintech business, and has an opportunity to provide feedback in that regard.

**Liam Flynn****Tel: +353 1 232 2025 / Email: liam.flynn@matheson.com**

Liam Flynn is a partner in Matheson's Financial Institutions Group. His practice focuses on advising financial institutions, especially banks and insurers, on strategically important matters, both transactional and regulatory. Prior to re-joining Matheson he was Deputy General Counsel of the Bank for International Settlements in Basel, the home of the Basel Committee on Banking Supervision. He is an officer of the IBA's Banking Law Committee and has advised and spoken on matters relating to cryptocurrency regulation, alternative/peer-to-peer lending and InsurTech.

**Lorna Daly****Tel: +353 1 232 3012 / Email: lorna.daly@matheson.com**

Lorna Daly is a senior associate in Matheson's Financial Institutions Group with broad experience in financial services regulation. Lorna is also a Prince2 qualified project manager. Lorna is Chair of the FinTech and Payments Association of Ireland's Regulatory Insights Group, and a member of the Irish Funds FinTech Working Group.

Matheson

70 Sir John Rogerson's Quay, Dublin 2, Ireland
Tel: +353 1 232 2000 / URL: www.matheson.com

Israel

Nir Porat, Roni Berkowitz & Ella Rosenberg
Porat Group

Introduction

Israel, as a jurisdiction, is widely known for its innovative ecosystem and for being the Middle Eastern Tech Hub. Apart from its vast futuristic and pioneering startup ecosystem, Israel also takes pride in a strong Innovation Authority which helps young entrepreneurs and enterprises to receive funding and gain a larger market foothold, in addition to a highly independent judiciary and justice system. Israel is a hybrid system of both Common Law and Civil Law, which is highly regarded; yet the regulation of Fintech has been predominantly slow and rigid for the past few years.

Being a state with a strong foothold in Fintech, it was expected that the Israeli Regulator would keep up with the global regulatory innovative advancements, yet this was not the case. There have been recent developments within the main financial regulatory bodies, but these developments do not cover the same scope or extensiveness of their global, and especially European, counterparts.

This ongoing global trend has had some impact in Israel. Israeli Fintech regulation is very slowly shifting from a densely codified set of rules and policies to an easier friendlier approach towards financial companies, and more specifically Fintech companies. This trend covers not only the regulatory institutions, but also recent judgments, innovation hubs and legislative initiatives.

This chapter will begin with approaches and developments of Israeli Fintech, then continue to cover the regulatory bodies in Israel, key regulations, restrictions, cross-border business and end with a conclusion.

Approaches and developments

Certain approaches and developments can be identified in the Israeli Fintech ecosystem.

First, it is vital to mention that the Fintech scene in Israel is thriving. Israel is blessed to have a very independent startup community. To that effect, the Israeli Regulator has decided to stay uninvolved in this industry and other industries, and let the companies develop themselves with very minor regulatory hurdles for company formation.

This minimum level of regulation of companies has contributed to a strong innovation presence in various industries. It is for this very reason that the Regulator, regardless of the industry, has maintained an almost neutral approach, which has proven to be the right decision. The vast cluster of companies in Israel has led to major developments, whether trade-related, financial or commercial, and has led to a boost to Israel's economy.

In addition to this minimum level of regulation, there is also a higher level of regulation per

field of operation. Each operational field or market in Israel has its own regulatory institution. High-risk operational fields in Israel are very highly regulated, regardless of the type of operation. The Israeli Regulator has taken the same approach when it comes to Fintech. For several years the Regulator has not touched upon Fintech for the preliminary reasoning of not fully comprehending what exactly blockchain and cryptocurrencies entail. Precisely for this *modus operandi*, the Fintech regulatory system in Israel has been left behind. A very unique situation has developed in which there are many Fintech companies and financial technologies that are mostly exported abroad, and the local market is left almost barren.

Several regulatory institutions in Israel, which each have their own mandate regarding certain market aspects, have recently understood the importance of a basic regulatory system for Fintech, developers and investors in the field.

This shift has resulted in the establishment of several additional institutions, jurisprudence and legislative bills, which shall be discussed in the following sections.

Regulatory bodies

Israel has five main regulatory bodies that regulate the Fintech sphere in Israel.

The Ministry of Finance (MOF), Bank of Israel, Ministry of Justice, Israel Securities Authority, Israel Money Laundering and Terror Financing Prohibition Authority have all demonstrated their concern with regards to Fintech, which has led to a highly regulated framework. Yet, those same institutions are currently working on easing the regulatory load. There is no coherent plan that one regulatory institution transcribes to the rest, but there is an operational collaboration between all the regulatory institutions.

For instance, The Ministry (MOF), in conjunction with other Israeli Ministries has recommended establishing a “*Regulatory Sandbox*” for the purpose of piloting Fintech startups with regulatory consultations and certain exemptions. This pilot, according to the Recommendation, will try to lift the stiff regulatory framework, consulting with jurisdictions that have already tried a similar pilot, such as Australia, Canada, Russia, the UK and the US. The Bank of Israel, on the other hand, has been held to very tight scrutiny by the local Fintech community. The Bank of Israel is Israel’s central bank and is the regulatory body that supervises the banks and their clients. The Bank of Israel handles complaints and deals with all legislative banking consumer bills that are forwarded to the Israeli Parliament (“*Knesset*”). Although the Bank is supposed to be the connecting institution between consumers, as well as Fintech companies in Israel, the Bank is under constant public scrutiny for not representing the Israeli Fintech scene well enough, and in some cases even going against its legislative mandate.

The Fintech business community in Israel has stated that in contrast to the vibrant financial hub, the Bank of Israel is not adhering to its own financial regulations and proving it impossible for companies to continue and develop their technology.

It was the same community that issued a letter to the Bank of Israel stating several issues that should be amended. The community’s plea is based on the “*Read Only*” Act or the Strom Act, which is supposed to enable Fintech companies to compete on a level-playing field with the banking groups in Israel, and lessen the grip of the same banking groups on the financial market, by giving those companies a licence to view the bank data on a “read-only” basis, without changing the content of the information on the bank servers.

The main argument is that there is lack of access to Fintech companies, which hinders competition by denying or postponing the following:

- Access to client information that is held by banks. There has been already a decision issued by the legislator to grant access to this information.
- Lack of full interface for Fintech companies and client data. This will be postponed until at least 2021.
- Opening bank accounts – current banking regulations makes it harder for Fintech companies to do so. This point has been recently ruled upon by the Israeli Supreme Court in *Bits of Gold v. Bank Leumi*.¹
- Issuing clear guidelines – the inter-ministerial committee issued guidelines that are too general.
- Providing a clear correlation between the actual needs of the interface and Fintech companies.

The Bank, in response, has stated that the reason it is not releasing the information or making the process of information access smoother is because the legal basis for this is flawed, and that this opinion is seconded by the Ministry of Justice and ISA – there are grave implications that may arise from opening the servers for companies, even if it is on a “read-only” basis.

The Ministry of Justice, trying to adhere to the current legislation, has an additional view on the matter, aside from the Strom Act.

Israel’s Ministry of Justice is the governmental office that is mandated by the Israeli Justice System, including the Judiciary, State’s Attorney and Prosecution. The Ministry of Justice’s approach towards Fintech, and specifically Israeli Fintech, has been deemed a very cautious approach, as it followed the lead of the other regulatory institutions in Israel. Yet, a very interesting shift has taken place within the past few months that is considered a premature legal Fintech earthquake.

A pioneering regulatory plan led by the Ministry of Justice, MOF and the Legal Advisor’s Office to the Government sets out a pilot framework for Israeli Fintech companies. This groundbreaking framework entails a reduced regulatory and compliance framework for Fintech companies, with certain taxation and disclosure benefits. Fintech companies who would be chosen for this pilot will have to provide sound business, innovation and technological plans. The pilot is ready to be lodged for a legislative procedure in the Knesset, yet due to the fact that the current government in Israel is a transition government awaiting elections, the Ministry of Justice has decided to halt the legislative procedure until the new government is sworn in. This pilot is in addition to the Ministry of Finance’s Fintech Lab.

National authorities, on the other hand, have a slightly better action plan than the Ministries. Israel’s Security Authority has been targeting a mixed approach when it comes to Israeli Fintech. The ISA stated in July 2018 that it will initiate an innovation hub targeted at the Fintech sector and companies. The reasoning behind this initiative, according to the ISA, is to keep the Israeli economy up to date with the latest financial developments, especially because the Israeli Fintech scene is mainly focused on the export of their services, rather than adhering to the local regulatory framework.

This initiative is not detached from reality, but rather the contrary. The ISA has reached an agreement with GFIN, which is the Global Financial Innovation Network. GFIN is mandated under the Financial Conduct Authority (FCA), and hails to increase financial innovation between states that are part of the Network, and to help consumers and Fintech companies reach better communication with local regulators.

In order to adhere to the proposed framework of GFIN, the ISA would need to provide relevance and added value; the innovation hub is at Israel's pioneering core.

Yet, this moderately novel tactic towards Fintech cannot be regarded as having a substantive tone. The ISA published an interim report in March 2018 in which it states the ISA's position on ICOs. The report claims to clear uncertainties regarding ICOs and Fintech, while trying to reassure investors and potential investors on the Fintech market and regulatory governmental services in Israel. The two main goals of the interim report were to explain how Israeli Securities Law applies to Fintech technology, and whether new amendments should be made to the current legislative act.

The interim report made a recommendation (Interim Recommendation) that cryptocurrencies should be deemed a *security* on a *case-by-case basis*, and not a *service*. This goes against the general approach of the EU, which has decided to let the Member States of the Union to decide on the definition of cryptocurrencies, and at the same time ignore the CJEU's ruling in *Hedqvist* that cryptocurrencies are exempt from VAT. This drastically different approach from the CJEU's ruling does not only prove that Israel's governmental institutions do not want to follow the lead of the EU, but want to set their own foothold in the Fintech realm.

With this, Israel is adopting a similar regulatory approach to Ireland, which also evaluates cryptocurrencies on a case-by-case basis and is currently waiting for the regulatory opinion of the EU institutions, and especially the EU Commission, on this matter.

At the same time, the Interim Recommendation sets a general rule regarding a right to a product or service. For the exclusive consumption use, cryptocurrencies will be deemed as a security. The same general rule also establishes that cryptocurrencies that will be used only for payments, exchange and/or clearing, are not limited to a specific venture, are not controlled by a central entity, and do not entitle additional rights, including *rights in rem*, and are not considered a security.

This very definition of the general rule above is one of the reasons that Israel needed the Recommendation, even though it is only a preliminary assessment of the status of the Fintech regulatory market in Israel. Unlike the EU, which takes pride in ESMA and other Member State-delegated agencies, and which has a very precise and clear-cut regulatory jurisprudence that restricts the use of cryptocurrencies in several Member States while enabling a wider range of crypto exchange in others, Israel's regulatory answer for years has been a deafening silence. This is because of the fact that until today, there has not been one legislative initiative that covers all Fintech regulatory aspects.

Key regulations and regulatory approaches

The Fintech offering in Israel is not only extensive, but it is also very diverse. Israel's unique innovative ecosystem, let alone its Fintech scene, is one of the most unique in the world, and can be regarded as a tech oasis in the Middle East.

Fintech in Israel is mandated under the following acts:

- Securities Act.
- Investment Advice Act.
- Regulated Financial Services Act.
- Companies Act.

In addition to the acts mentioned above, a very recent judgment issued by the Supreme Court of Israel has set the Israeli legal community in anticipation of further case law, as well as hopefully legislation to clear certain lacunas and harmonise the regulatory framework.

Bits of Gold settlement

The Supreme Court of Israel has ratified in a recent judgment a settlement agreement that was reached between Bits of Gold and Bank Leumi, in which the Bank agreed to adhere to the Supreme Court's recommendation, and allow Bits of Gold to maintain its bank account within Leumi for the use of digital assets.

This ratification by the Court, although a ratification of a settlement agreement, has a groundbreaking impact. Although it is not a ruling, such ratification, especially in light of the Supreme Court's recommendation, begs the inevitable question of the future of Fintech and cryptocurrencies in Israel.

The inescapable answer is that like all futuristic-related legislative initiatives and jurisprudence, the Fintech regulatory future in Israel is unknown. Be that as it may, the very recent ratification of the Supreme Court can be identified as a first step in the direction of a lighter grip of the regulatory belt on Fintech companies in Israel.

The remarkable point that this ratification emphasises is twofold. First, the Supreme Court of Israel, unlike the lower Courts (First and Second Instance Courts – Municipal and Regional Courts, respectively), took a different stand on the issue of Fintech and specifically digital assets. The Supreme Court, presided by Their Honors Dafna Barak-Erez, George Kara and Ofer GrossKopf, has decided to recommend Bank Leumi to accept a settlement, implying that a worse outcome may result if an agreement would have not been reached by the parties. This different approach has yet to be seen in Israel, which is regarded as rather slow when it comes to regulative advancements, especially in Fintech. Second, as regards a regulatory revolution, which has been widely anticipated and predicted by many actors in the field, this ruling can be seen as the first cornerstone to set.

Depending on the type of Fintech activity, most aspects are regulated. For instance, there is a difference between the type of governmental entity that mandates the specific regulation, whether it is the ISA or MOF; or there is a difference in the type of activity that is conducted. Furthermore, the Israeli Tax Authority announced in February 2018 that cryptocurrencies will be regulated and taxed as an asset, enabling the Israeli taxation system to tax those assets. This is in addition to the ISA's Interim Recommendation, and points again on the lack of uniformity between the regulatory institutions.

Restrictions

Israeli Fintech has seen many changes throughout the last few years. A vibrant ecosystem, which is comprised of technological companies, many of them being Fintech companies, can expect certain regulatory restrictions; yet those restrictions are still heavily imposed.

These restrictions on Fintech are mandated under the financial acts (Securities Act, Investment Advice Act, Regulated Financial Services Act, and Companies Act), and entail a 25% imposed tax on capital gains, and a 47% imposed tax on the marginal rate for businesses. These taxes are in addition to the mandatory 17% VAT, and lack of access of financial technological companies to information and the “*Read Only*” Act.

In addition, because the *Bits of Gold* ruling is not an ordinary judgment, but a ratification of a settlement agreement, it is not a binding precedent, and is not, yet, part of Israeli jurisprudence. Be that as it may, because the ratification was issued due to recommendations of the Supreme Court to Leumi Bank, it seems that the current presiding judges' opinion in the Court is leaning towards a less strict approach of banking and finance.

Cross-border business

Israeli Fintech is considered to be one of Israel's most unique exports. The Fintech ecosystem in Israel, and especially in the Tel Aviv Metropolis, is not only very rich in technology, but is also diverse and one of the very few markets in Israel that is primarily and predominantly exported. Due to this vast export of financial technology, and also tech companies, many of these Fintech enterprises wish to have their products adhere to and comply with the jurisdictional framework of each state. Due to this commercial approach, the European Union's regulatory framework has been widely sought after by Israeli companies.

Regulating financial products and services in the EU entails a very specific process, whether it is the licensing of cryptocurrency exchanges, or passporting of the licence. Complying with the EU's preliminary Blockchain Observatory and Forum Framework is not only a juridical condition to operate in the EU; it has become a *de facto* condition to facilitate many operational aspects of those companies in other jurisdictions, naming investments, especially for Israeli companies.

This cross-border relationship between Israel and the EU is one of the most unique trade relationships that can be identified in the field of Fintech. Israel's Foreign Trade Administration (FTA), oddly enough, has not dealt with this matter on a regulatory level. There is no specific policy for Fintech at the Israeli FTA, and the Export Institute adheres to the same methodology.

Be that as it may, both the Export Institute and Israel's FTA are heavily involved in marketing Israel's Fintech scene to the world. Both institutions are constantly showcasing Israeli companies around the globe.

The International Monetary Fund (IMF) has also caught up with the attractiveness of Israeli Fintech companies, and in a May 2018 report listed Israel's Fintech market as a dynamic tech sector, with a strong macro-economic presence and a healthy banking system. When discussing the risks that the governmental institutions are contemplating establishing in order to make Israel an attractive financial jurisdiction, the IMF notes important steps that Israel took in order to improve its position, compared to other countries, yet several more steps that should be taken. According to the IMF, a Financial Stability Committee is a critical condition in order for the Israeli economy and market to develop.

Second, the overwhelming majority (95%) of the banking industry in Israel is distributed between five banking groups, hindering competition. The IMF is increasingly making attempts to convince the Bank of Israel to open the sector to more competition. Fintech is one of those fields that the IMF is trying to impose on the Israeli monetary regulatory institutions and framework.

On a national level, the MOF has decided to promote the establishment of a Fintech-Cyber Innovation Lab, in collaboration with the Innovation Authority and the Cyber Directorate, for the purpose of increasing cross-border investment. The aim of this Lab is not just to open another investment route for Israeli companies, but also to showcase the developments that the Israeli Regulator has been transposing within the past few months. This will prove beneficial not only to the financial sector, but also to the regulatory bodies.

Conclusion

An estimated 400 Fintech companies operate from Israel. Most of them export their technology from Israel to other jurisdictions, mainly the European Union. The European

Regulator has a very clear set of rules and regulations, which are mandated by specific agencies and sub-agencies. The Israeli Regulator, on the other hand, has historically taken a different approach in regard to regulating high-risk markets, one of them being Fintech. There are several governmental institutions that regulate different aspects of Fintech. The Bank of Israel, Ministry of Justice, MOF, Israel Securities Authority, Israel Money Laundering and Terror Financing Prohibition Authority are all ministries and financial governmental institutions that issue regulations regarding Fintech.

Nevertheless, there is not a single legislative Act that encompasses Fintech as a regulated field in Israel. This issue has led to legal uncertainties and to undesired results, such as Israel not being considered a favourable jurisdiction for financial technological companies.

The reasoning behind the predicted setback in financial regulations stems from Israeli institutions' cautious approach in all innovative high-risk fields. When the Israeli Securities Authority was first approached by cryptocurrency companies, the Authority decided not to regulate simply because it did not understand the meaning of blockchain, and how it will affect the market indefinitely.

A question that gets frequently asked by many legal practitioners and Fintech experts in Israel is how and whether Israel has failed in keeping up with other markets and innovative regulatory legislative bills.

The answer certainly depends on the global regulatory spectrum. There are many jurisdictions, some of them being EU Member States, which have created a beneficial regulatory system that is very popular with Fintech companies, while some jurisdictions, such as China, have decided to ban cryptocurrencies as a whole.² There are even jurisdictions that have decided to collaborate with each other, such as the collaboration between United Arab Emirates (UAE) and Saudi Arabia for the creation of a new cryptocurrency.

When trying to locate Israel on the regulatory spectrum, it can easily be identified as a mid-range jurisdiction. On the one hand there is a very heavy regulatory load on Israeli companies with regard to taxation and policy submissions. On the other hand, there is a new realisation of the same regulatory bodies that the load should be lightened, and this has been demonstrated by the formation of new working groups and rulings of the Supreme Court.

When assessing the future of Fintech in Israel, a definite answer may not be given very easily. Yet, it is clear that the regulatory aspects of Fintech in Israel are heading towards a less rigid approach, while the justice system has given its first sign of trust in digital assets.

* * *

Endnotes

1. Discussed in the “Key regulations and regulatory approaches” section.
2. Except very narrow mining operations.



Nir Porat

Tel: +972 3 916 1661 / Email: Nir@porat.com

Nir is the founder and managing partner of the Porat Group. Nir has extensive in-depth knowledge in various fields of law, such as Commercial Law, Technology and Internet Laws, Blockchain and Cryptocurrencies, International Banking, Finance, Capital Markets, Payments, Litigation and Dispute Resolution, and Financial Technology. He is experienced in handling domestic and international complex transactions, as well as rendering ongoing corporate and commercial legal and business advice within Israel and in other jurisdictions. Nir has been representing and acting as legal counsel to a variety of multinational entities, providing them with comprehensive advice concerning all of their transactions, corporate, and business issues. Additionally, Nir is widely recognised as a leading specialist in the fields of Capital Markets, Fintech, Banking and Payments, Blockchain and Cryptocurrencies, and Gaming.



Roni Berkowitz

Tel: +972 3 916 1661 / Email: Roni@porat.com

Roni is a partner at the Porat Group, and is Head of the Financial Regulatory Department at the firm. Roni is the leading expert on Fintech in Israel. He has accumulated vast experience in the legal and commercial aspects of various online ventures, and has assisted many corporations and high-net-value private individuals operating in the global market with a particular expertise in the following fields: Affiliate Networks; R&D; Online Marketing; Trust Foundations; Bitcoin and Cryptocurrencies; Forex; Online Gaming; as well as numerous financial institutions dealing with the provision of online payments (credit cards processors, acquiring banks, EMI, PI).



Ella Rosenberg

Tel: +972 3 916 1661 / Email: Ella@porat.com

Ella is an EU Regulatory Consultant at the Porat Group, and the CEO of the Israel-EU Chamber of Commerce and Industry. A graduate of the European Law School, Maastricht University (LL.B. – EU Law) and Erasmus School of Law, Erasmus University Rotterdam (LL.M. – Commercial and Company Law). Ella is an EU Law expert, and focuses on EU Fintech, the EU Regulatory Framework, EU Common Commercial Policy, EU Blockchain, WTO Law and Israel's Foreign Trade Policy. She is the youngest CEO to be appointed to a Chamber of Commerce in Israel, and the first female CEO of the Chamber. Ella has lectured at PWC, DLA Piper, Tel Aviv Fintech Week, Israeli-British Business Club, Bit2C, held panels with ambassadors and lectured at various universities in Israel regarding the EU's Fintech Regulatory Framework.

Porat Group

Ha'arbaa Towers, South Tower, 24th fl, 30 Ha'Arba'a st, Tel Aviv 6473926, Israel
Tel: +972 3 916 1661 / URL: www.porat.com

Italy

Marco Penna, Marylisa Izzo & Gabriele Conni
Legance – Avvocati Associati

Approaches and developments

2018 was a decisive year for FinTech worldwide: global investments in FinTech companies exceeded the threshold of \$110 billion with more than 2,100 deals concluded. In this context, during 2018, investments in the FinTech industry in Europe reached \$34 billion, and the European economic scene has been characterised by the more than 500 deals which were concluded.

In general, 2018's global FinTech market was characterised by significant trends: (i) mobile technology allowed more and more people to use their mobile phones to access banking services; (ii) Initial Coin Offerings (“ICOs”) were emerging as a fundraising tool; (iii) insurance companies started distributing insurance products through technologies (so-called “InsurTech”), allowing them to create highly personalised insurance products; (iv) many banks and financial operators were developing business models without physical branches by distributing their services only through apps or online; and (v) internet giants (*i.e.*, Google, Amazon, Facebook, and Apple, also known as “GAFA”) have been playing a central role in the FinTech sector, gaining a significant position in the financial market. Just to mention a few relevant examples, Google has already obtained a banking licence in Ireland, while Amazon has been experimenting with some new forms of financing for its business customers. In this sense, considering the future development of technology and the potential that GAFA have in terms of funds they can invest to develop new technologies applied to finance, according to some observers, these international operators might replace traditional financial institutions and banks.

In Italy, FinTech is still less developed when compared to other leading countries. This notwithstanding, in terms of growth, the trends of the Italian market are extremely positive and lay a positive basis for the contribution to the international FinTech market. Indeed, the number of Italian FinTech operators has grown by 27% compared to 2017, and the turnover of the sector has also strongly increased in recent years.

In addition to the implementation in Italy of Directive (EU) 2015/2366 (so-called “PSD2”), through Legislative Decree No. 218 of 15 December 2017, an important event characterising the Italian market is the admission to trading of shares issued by a crowdfunding platform on the Italian stock exchange in March 2019 (*i.e.*, CrowdFundMe S.p.A.). Said company has been listed on the Milan Stock Exchange and managed to place 313,140 shares, after conducting 46 fundraising campaigns aimed at supporting start-ups.

As concerns FinTech regulation, although a uniform legal framework governing all aspects of this sector is still missing in Italy, the Italian legal system has been showing the first important signs of evolution in this area. In particular, a preliminary regulation in 2012 on equity crowdfunding has been gradually subject to changes in order to facilitate the development of the Italian crowdfunding market (this aspect will be further described below).

Moreover, also in light of the pressures coming from the European Parliament, Italy has recently distinguished itself from the other European States by providing the first juridical definition of Distributed Ledger Technology (so-called “DLT”) and smart contracts.

In addition, other new recently-issued provisions concern ICOs and blockchain, two areas that – as further specified below – have also caught the attention of the Italian supervisory authorities.

Finally, reference is made to the bill presented in March to the Italian Chamber of Deputies, which, on the basis of some information given by the press, should provide, *inter alia*, the legal basis for the creation of a regulatory sandbox for FinTech operators.

FinTech offering in Italy

The increase in the number of FinTech players and the access of some of them to the capital markets highlight the fact that FinTech is playing a central role in the present economy, and inevitably raises the question of whether traditional financial operators will lose their centrality in the provision of banking services (including collection of savings and lending activities).

This is even more true when considering the investment advisory service provided through the new robo-advisory technologies. In this respect, during the first part of 2017, the National Stock Exchange Commission (“Consob”) collected data and information concerning 10 operators providing investment services by using online robo-advisory platforms to produce a complete overview of the current status of the phenomenon in Italy (the report was issued in January 2019).

It is not easy to predict the future development of FinTech and say whether or not there will be a “disintermediation” of credit, but it seems likely that access to online finance is a real innovation as it allows families and small and medium-sized enterprises (“SMEs”) to obtain loans more easily. These new developments in the credit market should generate positive effects: in addition to cost and time savings, such innovations will probably constitute an additional boost to competition in the financial services market.

In light of the above, it seems necessary for States to adopt an adequate and complete regulation (primary and secondary) to guarantee the financial stability and legal certainty of the environment in which the new FinTech players may operate, so as to allow the further growth of a sector in which new technologies have already started to originate important developments.

Regulatory and insurance technology

Technological innovation applied to systems and procedures essential for banks to maintain compliance with regulatory requirements has recently reported significant progress in Italy. In view of the fact that compliance activities may also take advantage of new digital technologies, the Italian Banking Association (“ABI”) has set up a think tank in charge of carrying out in-depth studies in the RegTech sector. Having regard to the growing number of laws and over-regulation in the banking and financial sector over the last few years and the increase in banks’ statistical reporting requirements, it is easy to understand how essential it is to encourage the digital evolution of all these compliance activities. The think tank developed by ABI has the specific task of studying possible technological solutions that can facilitate compliance monitoring with the aim of reducing compliance costs incurred by the banking sector, thus improving the efficiency of the compliance processes. In particular, ABI’s RegTech think tank will focus on the automation and digitalisation of compliance controls through the use of algorithms, semantic search engines and AI solutions.

With respect to the application of new technologies to the insurance sector (*i.e.*, InsurTech),

several insurance companies are developing new systems of insurance policies underwriting as well as new insurance products. In particular, the use of smartphones and tablets has made it possible to spread micro-policies (*i.e.*, instant insurance contracts based on short-term coverage) in various sectors, including car sharing, home appliances, and sports activities. With reference to new insurance products, new technologies have made it possible to calculate the premium on the basis of an algorithm which, often using a blockchain logic, allows it to identify the different risk factors and to create tailor-made insurance policies.

The development of InsurTech is still modest in Italy and, therefore, although the Italian Insurance Authority (“IVASS”) has already shown its interest in analysing the phenomenon and interacting with InsurTech operators, the only (soft) law sources are to be found at an international level. Indeed, Italy has participated in a survey on “*Best practices on licensing requirements, peer-to-peer insurance and the principle of proportionality in an InsurTech context*” conducted by the European Insurance and Occupational Pensions Authority (“EIOPA”), who published their final report on 27 March 2019.

Key regulations and regulatory approaches

Current Italian legislation on FinTech

As mentioned above, in 2012 an equity crowdfunding discipline was issued in Italy, with provisions set forth in Legislative Decree No. 58 of 24 February 1998 and in Consob Regulation No. 18592/2013. In particular, according to the original version of these provisions, only innovative start-ups could have access to financing channels other than the traditional banking ones. Subsequently, through amendments to the aforementioned rules (see Law No. 232 of 11 December 2016 – the so-called “Budget Law 2017”), the number of entities having access to these alternative forms of financing was expanded to include all SMEs.

This extension has resulted in a strengthening of measures to protect investors (also due to the implementation in Italy of Directive (EU) 2014/65 – so-called “MiFID II”), and it has increased the supervisory powers of Consob on the activities performed by the crowdfunding portals. In this context, access to crowdfunding has been restricted to portals that adhere to a compensation scheme to protect investors and develop a more rigorous and detailed policy on conflicts of interest.

Finally, Law No. 145 of 30 December 2018 (the so-called “Budget Law 2019”) now allows SMEs to raise funds through bonds or debt instruments, provided that the offer is reserved to professional investors or particular categories of investors identified by Consob, and takes place within the limits provided by the Italian Civil Code.

On the other hand, with regard to DLTs and smart contracts, the Decree Law No. 135 of 14 December 2018 (converted into Law No. 12 of 11 February 2019) has introduced the definition of “distributed ledger technology” and “smart contract”, in line with the provisions issued at a supranational level. Noteworthy is the fact that the use of the DLTs produces the legal effects of the electronic time stamping referred to in Regulation (EU) 2014/91, and the smart contracts meet the requirement of written form after IT identification of the parties concerned. Indeed, this is the first *incipit* to the regulation of the matter – the Italian legislator has asked the Agency for Digital Italy to issue guidelines to specify: (i) the technical standards that the DLTs must possess in order to produce the legal effects of electronic time validation; and (ii) the process for identifying the parties who enter into smart contracts.

Innovation hubs, regulatory sandboxes and new forms of regulation

International regulation and, even more, European provisions impact the legal framework of those countries that have not yet regulated FinTech. In Italy, the regulation of the financial innovation sector in recent years has been based on the approaches followed at the international level: innovation hubs; regulatory sandboxes; and incubators. In this respect, the Bank of Italy, Consob and the IVASS have been particularly proactive. In particular, the Bank of Italy has adopted an innovation hub approach, which consists in the interaction of the Authority with the market players (*e.g.*, banks, financial intermediaries, start-ups) on all FinTech issues and at every stage. Such approach has allowed for the establishment of the FinTech Channel and the FinTech Unit within the Bank of Italy. The first was established in November 2017 and consists of a “hub” on the Authority’s website where operators may propose their own innovative financial projects, thus creating a dialogue aimed at supporting these processes. The latter is a department dedicated to dealing with the authorisations of new entities wishing to enter the financial market. Both the “hub” and the “Unit” constitute a privileged observatory on the orientations taken by the market.

Indeed, in May 2017 the Bank of Italy conducted a survey – the results of which are contained in the report published on the website of the authority in December 2017 – on the adoption of technological innovations applied to banking services. In particular, the report contains information on incentives and constraints relating to FinTech initiatives, as well as the investment programmes of interviewed market players.

On the other hand, the need to establish a productive discussion between the different Authorities prompted the Minister for the Economy and Finance to set up an internal coordination committee for FinTech on 17 March 2018. This committee is the result of a Memorandum of Understanding signed by the Ministry of the Economy and Finance, Bank of Italy, Consob, IVASS, Antitrust Authority, Guarantor for the Protection of Personal Data, Agency for Digital Italy and Tax Authority. In particular, the creation of the committee, which ensures coordination between supervisors, is a significant step towards the development of an overall vision of the FinTech sector in order to foster its growth and ensure adequate levels of consumer protection, stability and competition. As stated in the Memorandum of Understanding, the committee monitors the evolution of FinTech, identifies the areas of risk, and investigates regulatory and functional aspects, with a view to make proposals for a regulatory action. In addition, it enables cooperation and information exchange with the competent foreign institutions and conducts awareness-raising and communication activities on the Fintech issues of public relevance.

The same approach (*i.e.*, innovation hub) has been adopted by Consob in its role as authority with regulatory, informative and inspective powers for what concerns transparency and correctness of the operators’ behaviour when they offer investment services. In particular, upon the consultation document of 19 March 2019, a debate was launched at national level on the issue of ICOs and on the exchanges of crypto-assets (or tokens) in which Italian savers may invest: the Authority intends to receive, with a view to a subsequent public hearing, comments and proposals on – *inter alia* – the possible definition of these activities and the creation of a possible *ad hoc* regulatory framework.

In any case, Consob has pointed out the difficulties in defining crypto-assets, especially in the case of tokens whose yields are not clearly connected to ones having a financial nature: the latter is one of the elements characterising “financial products” pursuant to Italian law and Consob guidelines. According to Consob’s position, the only distinctive characteristics of crypto-assets are: (i) the use of innovative technologies, such as blockchain; and (ii) the

destination of the tokens to the subsequent negotiation, whose transferability is closely related to the technology used. Therefore, one of the solutions available to legally define crypto-assets should be creating an *ad hoc* category other than financial products. According to this case-by-case approach, the market or the Authority will evaluate each time whether the characteristics of the financial product are present or not.

The consultation document also proposes to describe the place where such crypto-assets are offered as “*an online platform whose exclusive purpose is the promotion and implementation of newly-issued cryptoactivity offers*”. As for the crypto-assets exchange systems, they would be defined as a set of rules and automated structures allowing for the collection and dissemination of the negotiation of crypto-assets proposals and to execute such proposals, including through technologies based on DLT. With reference to these systems, Consob proposes that only crypto-assets that have already been offered to the public on the platforms should be exchanged, provided that the system has been registered in a special register duly kept by the Authority.

Having said that, it seems appropriate to state that the Italian legislator is more and more interested in this sector. The foregoing has value especially considering the provisions set forth in the Budget Law 2019: it has been provided that a fund at the Ministry of Economic Development will be established in order to encourage the development of technologies and application of artificial intelligence (including blockchain).

Otherwise, the so-called “regulatory sandbox” approach, which allows FinTech operators to benefit from transitional regulatory derogations, has recently appeared on the Italian scene. On 14 March 2019, a bill was presented to the Chamber of Deputies on the digitisation of banking, finance and administration (Chamber Act No. 1673, not available yet). In particular, following the proposal of certain associations, such as AssoFinTech, the proposed law should allow, through the issuance of specific regulations, FinTech players to operate for a limited period of time, meeting lower capital requirements and complying with a simplifying regulation even without an authorisation. This is therefore the first small-scale trial of the derogation from the activity reserve, albeit limited in time.

SupTech

Finally, it is worth mentioning the innovation which has been affecting financial supervision (so-called “Suptech”): new digital technologies have an impact on the supervision carried out by the national supervisory Authorities (including, *inter alia*, the Bank of Italy). In this context, new technologies such as AI, as well as the availability of a huge amount of data (*i.e.*, big data), make it possible to improve the efficiency of the supervisory action performed by the competent Authorities. Just to give an example, the use of big data also makes it possible for the Bank of Italy to identify, through the use of complex techniques and algorithms (*e.g.*, machine learning), the correlation between the most common messages on social networks and the choices of deposit and investment made by banking customers, thus allowing them to better identify the financial stability risks. In any case, the use of such innovative applications is still in a primordial phase and it will therefore take time for this technology to be fully operational.

Restrictions

As far as companies operating in the FinTech sector are concerned, there are no particular regulatory restrictions applicable to them. In fact, it must be said that the application of the existing Italian banking and financial legislation does not specifically depend on how financial services are provided to the clients, but rather on the type of service provided. In this sense, the fact that the collection of savings and the lending activities are carried out through FinTech channels does not imply the application of a particular regulation.

**Marco Penna****Tel: +39 02 89 63 071 / Email: mpenna@legance.it**

Marco Penna is a Partner at Legance – Avvocati Associati. He has extensive experience regarding financial markets, with particular focus on investment services, securities offerings and off-site offerings. He regularly assists clients in relation to banking law, including regulatory capital and financial intermediaries incorporated under Article 106 of the Italian Banking Act. He has drafted agreements in relation to collective investment schemes, including UCITS and alternative investment funds, with specific reference to relevant shareholdings, shareholders activism and corporate governance. He has been involved in the incorporation of Italian asset management companies and collective investment schemes. He has provided assistance in relation to the regulatory profiles of banking, insurance and asset management M&A transactions. Marco Penna is mentioned in *The Legal 500* as a “*next generation lawyer*”. He speaks Italian and English.

**Marylisa Izzo****Tel: +39 02 89 63 071 / Email: mizzo@legance.it**

Marylisa Izzo is an Associate at Legance – Avvocati Associati. She is involved in banking law and focuses on banking regulation. She has taken part in securitisation and factoring transactions, and has also advised investment banks and European banking institutions in relation to European Financial and Banking Regulation. She speaks Italian, English and French.

**Gabriele Conni****Tel: +39 02 89 63 071 / Email: gconni@legance.it**

Gabriele Conni is an Associate currently practising in the Financial Intermediaries Regulation department.

Legance – Avvocati Associati

Via Broletto, 20 – 20121, Milan, Italy
Tel: +39 02 89 63 071 / URL: www.legance.com

Japan

Ken Kawai, Shunsuke Aoki & Keisuke Hatano
Anderson Mōri & Tomotsune

Approaches and developments

There has been a series of significant Fintech-related changes to the regulations in Japan. We note that most of those changes are driven by the regulators' intention to stimulate Fintech business and innovations in legacy financial institutions in Japan. Additionally, regulators have had to deal with various consumer protection issues that have arisen in Japanese Fintech industries, which resulted in their decision to strengthen the regulations governing emerging Fintech businesses in order to address new risks for consumers arising from the new services. We set forth below typical cases of this regulatory trend in Japan.

Crypto assets

Japan was the first country to establish a regulatory framework for crypto assets. The crypto asset market in Japan experienced exponential growth in 2017 on the coattails of a steep rise in the price of Bitcoin and growing enthusiasm for initial coin offerings (“ICOs”). Japan has emerged as one of the largest crypto asset markets globally.

In January 2018, however, one of the largest crypto asset exchanges in Japan announced that it had lost approximately USD 530 million worth of cryptocurrencies in a hacking attack on its network. Thereafter, the Financial Services Agency of Japan (the “FSA”) began performing on-site inspections of registered exchanges and deemed registered exchanges (which conduct business on a temporary basis), including the hacked exchange. On March 8, the FSA announced that it ordered two deemed exchanges to suspend their business and two registered exchanges plus three deemed exchanges to take specific steps for business improvement. The regulatory landscape surrounding crypto assets in Japan will drastically change once the bill developed in response to the hacking incident passes into law. Please refer to “**Key regulations and regulatory approaches**” below for details.

Open APIs

Open APIs are another trend for the Fintech business operators in Japan. In March 2017, the Diet passed a bill amending the Banking Act to regulate “electronic payment intermediate service providers” to facilitate open APIs (Application Programming Interface). The amendments, including relevant subordinate regulations, went into effect on June 1, 2018. Under the amendments, financial institutions must adopt and make public the standards for decisions to enter into contracts with specific electronic payment intermediate service providers (please refer to “**Key regulations and regulatory approaches**” below for the definitions and related regulations for electronic payment intermediate service providers). Financial institutions must treat electronic payment intermediate service providers that meet such standards in a fair and non-discriminatory manner. Financial institutions intending to enter into contracts with electronic payment intermediate service providers are required to

make efforts to develop an open API system by the end of May 2020. According to a survey conducted by the FSA in March 2019, more than 130 banks operating in Japan have made open or are planning to open their APIs to Fintech companies. New businesses in collaboration with banks and Fintech companies utilising the open APIs are expected to be created.

We believe this trend will not change over the next few years, as there are other areas such as mobile payment services where Fintech services are expanding rapidly and the Financial System Council (the “FSC”), the advisory body for the Japanese government, is continuing its discussion for drastic reform of the financial regulations.

Fintech offering in Japan

In Japan, crypto asset-based businesses, cashless payment or mobile payment services, financial account aggregation services, robo-advisors, and crowd funding are relatively active Fintech offerings. Meanwhile, innovation of peer-to-peer lending and InsurTech is yet to come.

It was notable in 2018 that an increasing number of companies entered into or expanded their businesses in the mobile payment market. It is often stated that Japanese citizens highly prefer cash payment and that the prevalence of cashless payment is much lower than in other major economies. According to the report “Cashless Vision and API Guidelines for Utilization of Credit Card Data” released by the Ministry of Economy, Trade and Industry of Japan (the “METI”) in April 2018, the ratio of cashless payment in Japan was less than 1:5 (20%) in 2015. However, in 2018, quite a few companies launched QR code payment services, and they are currently facing great competition. Fintech ventures such as Origami and PAY, and IT platforms such as Rakuten, Line, Yahoo, and NTT Docomo have already launched QR code payment services.

As a counter movement to these disruptive expansions of mobile payment services provided by newcomers from outside of the financial industry, in March 2019, Mizuho Bank, which is one of the Japanese “Mega Banks”, accompanied by more than 60 regional banks, launched a QR code payment service named “J-Coin Pay”.

From a legal perspective, these QR code services fall within three models: prepaid; direct debit payment; and deferred payment. The prepaid model requires a user to transfer funds from a bank account prior to a payment. The deferred payment model requires a user to link an existing credit card to the QR code application. Both models are relatively common in Japan, and the direct debit payment model is less popular but has been expanding recently. As different regulations apply to each model, entities seeking to undertake business related to QR code payments in Japan are recommended to consult a regulatory specialist for compliance purposes.

Regulatory and insurance technology

RegTech has not yet come to Japan; however, the FSA officially announced in its Assessments and Strategic Priorities 2018 that it would enhance RegTech and SupTech (Supervisory Technology) in Japan. One of the recent legislative changes in this area is that, in 2018, the subordinate regulations of the Act on the Prevention of Transfer of Criminal Proceeds were amended in order to finally make several methods of e-KYCs available in Japan.

InsurTech appears to still be behind other areas of Fintech, such as payment and crypto assets businesses in Japan. While quite a few Japanese insurance companies appear to be interested

in InsurTech and, therefore, either attempt to develop their own InsurTech tools or invest in overseas InsurTech enterprises, we have not seen many InsurTech startups in Japan so far.

Regulatory bodies

There are several relevant regulatory bodies for Fintech businesses in Japan.

A firm (including an overseas firm) that wishes to undertake regulated activities in Japan is required to obtain the applicable licence from Japanese financial regulators, the FSA or one of the Local Financial Bureaus that the FSA has delegated a part of its authority to, except for services related to deferred payments, which require authorisation from the METI.

Fintech-related laws such as the Banking Act, the Payment Services Act (the “PSA”) and the Installment Sales Act incorporate regulations addressing both prudential supervision and consumer protection. As a result, a regulator who governs each act will be a single regulator from the perspective of both prudential supervision and consumer protection.

Key regulations and regulatory approaches

Crypto asset-related services

Regulations on cryptocurrency came into force on April 1, 2017. The PSA was amended to introduce registration requirements for “crypto asset exchange service providers”. For purposes of the PSA, “crypto asset” is defined as:

- i. proprietary value that may be used to pay an unspecified person the price of any goods purchased or borrowed or any services provided, where such proprietary value may be (a) sold to or purchased from an unspecified person, provided such sale and purchase is recorded on electronic or other devices through electronic means, and (b) transferred through an electronic data processing system; or
- ii. proprietary value that may be exchanged reciprocally for such proprietary value specified in the preceding item with an unspecified person, where such proprietary value may be transferred through an electronic data processing system.

Most of the so-called payment tokens and utility tokens would fall within the definition of a crypto asset.

Crypto asset exchange services have been defined to include any of the following acts carried out as a business:

- i. the sale/purchase of crypto assets or exchanges for other crypto assets;
- ii. intermediary, agency or delegation services for the acts listed in (i) above; or
- iii. the management of users’ money or crypto assets in connection with the acts listed in (i) and (ii).

As a consequence of this definition, not only typical crypto asset exchanges, but also so-called OTC brokers, are regulated as crypto asset exchange service providers under the PSA. Moreover, most ICOs or token sales fall within the definition of crypto asset exchange services. As a result, a token issuer must, as a general rule, be registered as a crypto asset exchange services provider if the token sale (i.e., the ICO) is targeted at residents in Japan. Notwithstanding the foregoing, it has been argued that a token issuer does not need to undergo registration as a crypto asset exchange service provider if the issuer has completely outsourced its token issuance to a reliable ICO platform provider that is registered as a crypto asset exchange services provider.

It should be noted that the legal framework regulating crypto assets will likely change significantly in 2019 and 2020 due to the bill responding to the hacking incident mentioned in “**Approaches and developments**” above, although the definition of crypto asset will not change. On March 2019, the FSA submitted a bill to the Diet for the revision to certain legislation governing crypto assets. The following is a summary of the key revisions proposed:

- i. Inclusion of additional regulations on crypto asset custody services.
- ii. Tightening of regulations governing crypto asset exchange services.
- iii. Establishment of “electronically recorded transferable right” (the “ERTR”) and application of regulations thereto.
- iv. Introduction of regulations governing crypto asset derivative transactions.
- v. Introduction of regulations governing unfair acts in crypto asset or crypto asset derivative transactions.

The bill will come into force within a year of its introduction upon its passage by both chambers of the Diet.

One of the noteworthy developments in the regulatory framework of crypto assets businesses proposed under the bill relates to so-called security tokens. In this area, Japanese regulators have been unclear on whether “initial coin offerings” (“ICOs”) and “security token offerings” (“STOs”) are governed by the PSA or the FIEA, or both. For this reason, prospective issuers (including overseas issuers) of ICOs and STOs in Japan have faced significant uncertainty. This has resulted in the restriction of ICO and STO issuances in Japan. To address this situation, the bill introduced the concept of the ERTR to clarify the scope of security tokens governed by the FIEA. More specifically, the ERTR is defined to include tokens representing rights where distributions are paid to token holders on the profits of the business conducted by the token issuer, and calculated based on the ratio of the holder’s token ownership. Consistent with this, the bill also excludes ERTRs from the definition of “crypto asset”. Accordingly, it is now clear that the PSA is inapplicable to tokens falling within the definition of ERTR.

Electronic payment intermediate service

On June 1, 2018, the amendment to the Banking Act came into force to regulate electronic payment intermediate service providers in order to facilitate open APIs. Electronic payment intermediate service providers are defined broadly enough to include intermediaries between financial institutions and customers, such as entities using IT to communicate payment instructions to banks based on entrustment from customers, or entities using IT to provide customers with information about their financial accounts held by banks. Entities providing financial account aggregation services are also categorised as electronic payment intermediate service providers. They are required to register with the FSA in order to provide these services.

Below are the key regulations applicable to registered electronic payment intermediate service providers:

- i. An electronic payment intermediate service provider that intends to conduct services that constitute electronic payment intermediate services must, in principle, disclose certain matters in advance. Such matters include the tradename or address, authority, indemnity, and the contact details of the office dealing with complaints.
- ii. With regard to electronic payment intermediate services, electronic payment intermediate service providers must: (a) provide information to prevent misunderstandings; (b) ensure proper handling of user information; (c) ensure safety management; and (d) take measures to manage outsourcing contractors.

- iii. Electronic payment intermediate service providers must conclude a contract regarding electronic payment intermediate services with a bank prior to performing acts that constitute electronic payment intermediate services.
- iv. The contract must specify (a) the allocation of indemnity liability in cases where users suffer damage, (b) measures for proper handling of user information, and (c) measures for safety management. Both the bank and the electronic payment intermediate service providers must publish (a) to (c) above without delay when concluding the contract.

Other services

Apart from the regulations applicable to crypto asset exchange services and electronic payment intermediate services, there is no regulatory framework specifically designed to regulate Fintech businesses in Japan. However, if the services provided by the Fintech companies are subject to existing financial regulations, they are required to comply with these regulations, which include obtaining any applicable licence. A firm (including an overseas firm) that wishes to undertake regulated activities in Japan is required to obtain applicable authorisation from Japanese financial regulators, the FSA or one of the Local Financial Bureaus to which the FSA has delegated a part of its authority or the METI. Please note that if an entity conducts solicitation in Japan for using its services, even if this is done from abroad, such act is considered to be an undertaking of activities in Japan.

Money transfer services are regulated under the Banking Act and acts applicable to other depository institutions, which require those who wish to enter into this business to obtain the relevant licence from the FSA; provided, however, that the service of a money transfer of not more than JPY 1 million can be provided if a firm obtains registration as a “funds transfer service provider” under the PSA.

Regarding e-money, the issuer of e-money must comply with the applicable rules under the PSA. If e-money can be used only for payments to the issuer for its goods or services, the PSA does not require the issuer to obtain registration, provided that they comply with some reporting obligations. On the other hand, if e-money can be used not only for payments to the issuer for its goods or services but also for payments to other entities designated by the issuer, then the issuer is required to obtain registration as an “issuer of prepaid payment instruments” under the PSA.

Please note that an online payment instrument can be considered either as a “funds transfer” system, a “prepaid payment instrument”, a “crypto asset” or something else. As the scope of each type of payment instrument is not easy to distinguish, it is recommended to consult specialists if an entity wishes to undertake business related to online payments in Japan.

Influence of supra-national regulatory bodies

The Financial Action Task Force has been influential in the development of Fintech-related regulations in Japan. For instance, the Guidance for a Risk-based Approach to crypto assets by the Financial Action Task Force (FATF Guidance) in June 2015 was the trigger for the introduction of regulations on crypto asset exchanges in Japan. The introduction of regulations on crypto asset custody service, which we mentioned in “**Key regulations and regulatory approaches**” above, was pursuant to the recommendation of the Financial Action Task Force in October 2018.

Additionally, the introduction of a risk-based approach to the AML guideline of the FSA, published in February 2018, was also a reaction to the FATF recommendations.

Financial regulators and policymakers in Japan are receptive to Fintech innovation and technology-driven new entrants in the regulated financial services markets, provided that

the FSA is taking a more conservative approach than before to cryptocurrency-based businesses following the hacking incident mentioned above in **“Key regulations and regulatory approaches”**.

Sandbox and other initiatives

In June 2018, the Headquarters for Japan’s Economic Revitalization, under the Cabinet Secretariat, opened a cross-governmental one-stop desk for the regulatory sandbox (the “Regulatory Sandbox”) within the Japan Economic Revitalization Bureau. The Regulatory Sandbox can be used by Japanese and overseas companies, and it enables companies that apply and receive approval for projects not yet covered by present laws and regulations to carry out a demonstration under certain conditions without the need for amendment of existing laws or regulations. There is no limitation on the area of business regarding which companies can apply for the Regulatory Sandbox; however, AI, IoT, big data and blockchain projects are explicitly mentioned as the most prospective and suitable areas.

Separately, in December 2015, the FSA established the “Fintech Support Desk”. It is a one-stop contact point for inquiries and exchange of information on Fintech. It accepts a wide-range of inquiries on various matters from those who currently operate Fintech businesses and others who intend to start Fintech startups.

In addition, the FSA established a “Fintech Experiment Hub” in September 2017. The Hub gives support to Fintech companies and financial institutions when they conduct an unprecedented Proof of Concept (“PoC”). Please note that certain regulations are not suspended during the PoC, but the Hub aims to eliminate companies’ concerns of violating applicable regulations during the PoC by providing legal and other advice.

In March 2017, the FSA announced the launch of the “Financial Market Entry Consultation Desk” to give advice on Japan’s financial regulations to foreign financial business operators that plan to establish a Fintech business based in Japan.

Restrictions

There are, at present, no prohibitions or restrictions that are specific to Fintech businesses in Japan. Certain types of Fintech business are regulated (see section above), but these businesses can be carried out in compliance with applicable regulations.

As we noted in **“Key regulations and regulatory approaches”**, a remarkable recent topic with respect to restrictions is, the hacking of the crypto asset exchange, which triggered revisions of the regulations governing crypto assets and crypto asset exchanges.

Cross-border business

It is worth noting that some Fintech players in Japan are collaborating with global payment businesses. For instance, Line Pay and PAYPAY, both emerging QR code payment service providers in Japan, are collaborating with Tencent and Alibaba, respectively, enabling merchants in Japan to receive payments by We-Chat Pay and Alipay. Additionally, there are some international fund transfer service providers licensed in Japan who are providing overseas fund transfer services using their own fund remittance infrastructure at a reasonable cost compared to traditional banks.

In March 2017, the FSA and the UK’s Financial Conduct Authority jointly announced that they exchanged letters on a co-operation framework to support innovative Fintech companies in Japan and the UK to enter each other’s market by providing a regulatory referral system. The FSA has established similar frameworks with the Monetary Authority of Singapore

(“MAS”), the Australian Securities & Investments Commission (“ASIC”), the Abu Dhabi Global Market Financial Services Regulatory Authority (“ADGM”), and the Swiss Financial Market Supervisory Authority (“FINMA”).

The Tokyo Metropolitan Government (the “TMG”) released a paper titled “Global Financial City: Tokyo Vision – Toward the Tokyo Financial Big Bang” in 2017. While it outlines various measures to nurture domestic players and attract foreign players throughout the financial sector, the TMG gives particular importance to asset management and Fintech businesses and sets its aim to attract 40 foreign asset managers and Fintech companies by fiscal year 2020.

As a part of such measures, the TMG opened the “Business Development Center Tokyo”, which offers foreign entrepreneurs who are considering an expansion of their businesses in Tokyo a total support package covering all aspects from business through to lifestyle issues. For foreign companies planning expansion into the Special Zone for Asian Headquarters in particular, the Center provides both business exchange support and specialised consulting services. Furthermore, the “Tokyo One-Stop Business Establishment Center” facilitates the incorporation of its ancillary procedures, such as taxes, social security, and immigration for foreign entrepreneurs considering establishing businesses in Tokyo.



Ken Kawai

Tel: +81 3 6775 1205 / Email: ken.kawai@amt-law.com

Ken Kawai has extensive experience advising financial institutions, Fintech startups, investors and corporate clients on complex finance and financial regulatory matters. Ken focuses primarily on the Fintech industry and regularly advises Fintech companies, financial institutions, international organisations and industry organisations on legal issues surrounding Fintech, including the complex legal framework governing cryptocurrencies and blockchain.

Ken also specialises in derivatives and has counselled global banks, broker-dealers and investors on regulatory matters and best practices with respect to derivatives and related products. Ken's deep and practical knowledge in this area is rooted in his 17-year career at MUFG Bank, Ltd. (formerly known as the Bank of Tokyo-Mitsubishi and, prior to that, the Bank of Tokyo Ltd.), where he was involved in derivatives trading and marketing.



Shunsuke Aoki

Tel: +81 3 6775 1173 / Email: shunsuke.aoki@amt-law.com

Shunsuke is a partner at Anderson Mōri & Tomotsune. Since joining the firm in 2008, Shunsuke has been primarily engaged in financial regulatory matters with recent particular focus on Fintech matters, corporate finance transactions including equity and debt offerings in both domestic and international capital markets, and project finance transactions. Shunsuke has external experience at one of Japan's leading securities houses (2014–2016) where he was a member of the Capital Market Department in the Investment Banking Division, and at Sullivan & Cromwell LLP, New York (2013–2014) as a Visiting Lawyer. Shunsuke is admitted to practise in Japan and New York and earned a J.D. from University of Tokyo School of Law and an LL.M. from New York University School of Law.



Keisuke Hatano

Tel: +81 3 6775 1250 / Email: keisuke.hatano@amt-law.com

Since joining the firm in 2011, Keisuke Hatano has been involved in a number of significant finance transactions. He has extensive experience advising financial institutions and Fintech companies on regulatory matters.

In addition to his professional experience at Anderson Mōri & Tomotsune, he worked for the Financial Services Agency where he was mainly engaged in two separate processes of amending the Banking Act in 2016 and 2017 with the aim of creating a pro-Fintech environment for a second consecutive year.

Anderson Mōri & Tomotsune

Otemachi Park Building, 1-1-1 Otemachi, Chiyoda-ku, Tokyo 100-8136, Japan

Tel: +81 3 6775 1000 / URL: www.amt-law.com/en

Korea

Won H. Cho, Hye In Lee & Hyeseon Han
D’LIGHT Law Group

Approaches and developments

Fintech, the term introduced and created by combining the words finance and technology, is no longer a new or innovative concept to us. Considering that the term refers to the adoption of information and communication technology to improve accessibility and speed of finance services, the word is almost perfectly self-explaining. Although Korea is well-known for the world’s top-level internet network infrastructure and smartphone penetration rate, development of the fintech industry was slow due to strict financial regulations. As fintech became a global trend, the government started to encourage the development of fintech by amending legislation and benchmarking foreign fintech players.

In August 2013, the Financial Investment Services and Capital Markets Act (the “FISCM Act”) allowed for the adoption of a robo-advisor in discretionary investment businesses, which are businesses managing and operating, at their own discretion, an investor’s financial assets considering such investor’s purpose of investment or financial status. A robo-advisor is required to satisfy certain conditions on the part of the investor, such as the direct analysis of an investor’s propensity, their investment in at least two items, the readjustment of their portfolio in every quarter, their evaluation by qualified external experts and more, in order to give advice on investment and manage assets. In April 2019, the FISCM Act extended the range of the business covered by robo-advisors to collective investments businesses, which manage assets pooled by inviting two or more persons.

2015 was a boom year for internet banks and easy payment in Korea. In June, the Financial Services Commission (“FSC”) announced that it will start to give permission to internet banks which provide banking services through electronic apparatus in a non-facing and automated manner; three such entities applied for internet bank permission in October. Two out of three applicants, the K Bank and the Kakao Bank, finally passed the tests and started business in 2017. The frontiers had to meet all the conditions and qualifications for conventional banks under the Banking Act, but the Special Act on Establishment and Operation of Internet-Only Banks (the “Internet-Only Bank Act”) was enacted in 2018 to lower the hurdles further. Further, in March 2015, the authorised certificate, which has been long criticised as a major hindrance to the development of Korean fintech technology and the market, became non-mandatory in the electronic financial transaction. As a result, Korea’s major corporations such as Samsung, Naver, SK, Shinsegae, and Lotte each and separately rushed to launch their own easy payment application in 2015. Now, the Korean easy payment application market is very competitive, with more than 50 applications.

Application of the blockchain, one of the hottest and innovative fintech ideas, to the Korean financial market is being discussed and sought in various ways. For example, a blockchain-

based certification system is being developed to substitute the conventional authorised certificate and a blockchain based local currency called No-Won Coin was launched and is currently in use. Further, numbers of “altcoins”, which refers to cryptocurrencies other than Bitcoin, and cryptocurrency exchanges have newly appeared. It is no secret that cryptocurrency has been a hit in Korea and a massive amount of cryptocurrency transactions were made in the last two years. Now, the Korean government is planning to announce regulations on taxation of cryptocurrencies, ICO, and more.

Fintech offering in Korea

The easy payment system has been the most competitive and disrupting item to enter the Korean traditional financial services market. A survey showed that in 2017, only 24.3% of transactions were made in cash and 41.3% were made by credit card. The Korean credit card system is based on the so-called “three party model” in which a credit card issuer also acts as a credit card acquirer at the same time. A credit card issuer should issue credit cards to customers, recruit merchants, review and approve each request for payment from merchants, pay such amounts to merchants, gather and process bills for transactions so far made between merchants and customers, and collect such amounts from respective customers.

Because the burden of a credit card issuer is so high and costly, credit card issuers started to delegate credit card acquirer transaction processing works to a Value Added Network (“VAN”), and VANs soon became a unique and customary practice in the Korean traditional credit card market. In 2015, the Specialized Credit Finance Business Act (the “SCFB Act”) was amended to govern VAN business. The Electronic Financial Transactions Act (the “EFT Act”) is also applicable to VANs but it does not impose any meaningful obligation on VANs. VANs recruit merchants on behalf of credit card issuers, provide payment terminal devices and network to merchants, transfer requests and approval for payment between merchants and credit card issuers, and collect, categorise and report bills to credit card issuers so that they can collect such amount from the customers. In return, VANs receive fees from credit card issuers. VANs did reduce the cost and improve the service quality when the network and system for credit card was poor, but now the needs of VANs are decreasing and even being criticised as the reason for the rise of fee rates related to credit card payments.

In online markets, Payment Gateway (“PG”) steps in. PG recruits merchants, stores and confirms customers’ credit card and personal information, and transfers requests and approvals for payment between merchants and credit card issuers, and collects, categorises and reports bills to credit card issuers through VANs. The difference is that PG contracts directly with merchants, and with credit card issuers as representatives of merchants. There is no direct contractual relationship with merchants and credit card issuers. Thus, merchants pay fees to PG, not credit card issuers, and PG pays fees to credit card issuers. Because PG still deals with credit card issuers through VANs, PG disrupts VANs but does not completely replace them. PG is governed under the EFT Act, and is also regulated under the SCFB Act as a merchant.

As the online market and the number of smartphone users grew rapidly, security became a huge issue, because customers have to input a large amount of critical information such as credit card numbers, expiry dates, passwords and social security numbers for online transactions. Further, the mandatory use of the authorised certificate, together with the heavy Active X security program in online shopping mall transactions exceeding approx. 300 USD, of internet banking, was slowing down the speed of online transactions and making online

shopping less attractive to users. Consequently, the easy payment system appeared, which enables online payments using an online ID and password after credit card information is registered. VANs, PG, credit card issuers and new fintech companies have been striving to develop new easy payment systems, and competition intensified after the mandatory use of the authorised certificate was abolished. And now, the App-to-App Payment system, which transfers money from a user's account to the other user's account directly, is being named as a payment system to replace credit card payments. The App-to-App Payment system has merits over traditional credit cards on various points. It has a lower fee rate – almost a quarter of that of credit cards, as PGs and VANs do not intervene in the payment process, the recipient does not need to download the application or have payment terminals, and transactions can be made between private persons.

Toss and Kakaopay are the leading App-to-App Payment service providers, and the Korean government launched the Zero Pay platform beta version in December 2018. Zero Pay is a QR-code transaction platform introduced by the Seoul Metropolitan Government to lighten the financial burden on small businesses by avoiding credit card fees. The Korean government is encouraging the use of Zero Pay, offering tax benefits. If App-to-App Payment successfully takes market, then VAN, PG, and credit card issue business will be disrupted greatly. However, one should not be too optimistic about App-to-App Payment, as it is a system fundamentally based on debit payment of which payment can be made up to the bank balance, making it much less attractive to people who are used to the credit card system.

Regulatory and insurance technology

RegTech is a word created by combining regulatory and technology. It is a service which enhances the regulatory process by utilising technologies such as artificial intelligence (“AI”), blockchain, big data and cloud computing. For example, RegTech can collect and analyse big data in relation to credit card transactions, share data and report to authorities through cloud computing and store data using blockchain, and have AIs monitor transactions in real time.

The Korean government has consistently manifested its willingness to encourage financial companies to develop and adopt RegTech since 2017, and launched the RegTech Development Council in October 2018 accordingly. The Council announced that RegTech is the breakwater which blocks risks from fintech innovation waves, and it will construct infrastructure to enhance the development and use of RegTech. Also, it will run a pilot test for Machine Readable Regulation, which translates financial regulations to machine language, starting from the EFT Act.

The Financial Security Institute, a financial security-specialised organisation founded to create a safe and reliable financial environment and to contribute to the establishment of a convenient financial environment for financial consumers and financial institutions, launched a RegTech platform in January 2019. This platform provides an automated compliance management service, an automated financial security reporting service, a search and notice service on intelligence regulation, and financial security support.

InsurTech is a combination of the words insurance and technology, and which refers to the utilisation of technology to make the insurance industry cheaper and more efficient. A few pieces of legislation are obstacles to InsurTech in Korea. The first relates to the separation of industrial and financial capital. Insurance companies cannot have fintech subsidiaries, so they can develop InsurTech only by partnership with fintech companies. The Medical Service Act strictly limits the medical service to be provided by doctors, nurses and other

qualified medical persons. Some InsurTechs analyse health data, discount premiums based on such health information, and provide health information to the insured. Because such analysis and notification may be construed as diagnosis, which is a medical service, it is risky to operate such types of InsurTech in Korea.

Further, there are other regulations making certain InsurTechs which are active in other jurisdictions unavailable in Korea. Yet regardless of such restrictive regulation, insurance companies are starting to introduce InsurTech. For example, robotic process automation learns the patterns of how computer documentation works and automatically writes reports, manages contracts and such. The company Dentinote makes the insured take a picture of his or her teeth to check their condition, and the insurance company discounts premiums in return. But still, InsurTech in Korea remains at a premature level.

Regulatory bodies

In general, the FSC and the Financial Supervisory Service (the “FSS”) are the major regulatory authorities in the fintech industry. The FSC is the government regulatory authority which assumes primary responsibility for rulemaking and licensing, while the FSS principally conducts supervision of the financial industry, including prudential supervision, capital market supervision, consumer protection, and other activities delegated by the FSC. Although the FSS is an organisation under the FSC, which is a governmental body, it is not itself a governmental body. The FSS is a specially legislated supervisory authority staffed by private sector employees who are not part of the government civil service system. This two-tier system is devised to reduce the risk of the government attempting to deprive the freedom and take control of financial companies.

The FSC has the statutory authority to draft and amend financial laws and regulations and issue regulatory licences to financial institutions. For example, anyone who wishes to run an internet banking business should obtain permission from the FSC under the Banking Act following the detailed procedure and conditions decided and announced by the FSC. Similarly, the FSC has the authority to give a licence for a robo-advisor business under the FISCMA Act and an easy payment business under the EFT Act. In addition, the FSC supervises foreign exchange transactions and leads the government’s anti-money laundering and counter-terrorism financing efforts.

Prudential supervision is the main objective of the FSS. The FSS regularly carries out both targeted and full-scope examinations to evaluate financial firms’ financial health, risk management, internal controls, management competence, and compliance with rules and regulations. Consumer protection is another goal of the FSS. The FSS provides consumer complaint resolution services and consumer education programmes. Consumers can file complaints with the FSS against financial services firms through the consumer complaint resolution service and seek mediation and resolution. Because the FSS is more focused on prudential supervision than consumer protection, new legislation for consumer protection and the establishment of a separate organisation specialised for consumer protection thereunder has been long discussed, but it has not been ratified yet.

Key regulations and regulatory approaches

The regulations regarding fintech in Korea can be classified into the following topics:

- **Banking business:** the Banking Act deals with inherent banking business, which is defined as business with lending funds raised by bearing debts owed to many and

unspecified persons, by the receipt of deposits or the issuance of securities and other bonds; while the Internet-Only Bank Act, introduced in September 2018, includes special regulations for internet-only banks that mainly conduct banking business via electronic financial transactions. The special rules included in the Internet-Only Bank Act are as follows: first, any person who intends to obtain authorisation for banking business shall have capital of at least 100 billion KRW (provided that a local bank's required capital may be at least 25 billion KRW); while internet-only banks only require 25 billion KRW. Second, a non-financial business operator may hold up to 34% of the total number of outstanding voting stocks of a bank, instead of 4% (with some exceptions) as stipulated in the Banking Act, as the Internet-Only Bank Act eases the restrictions on stockholding by non-financial business operators. The restrictions on stockholding by non-financial business operators intend to prevent the non-financial sector from controlling the financial sector, but have hindered convergence and innovation between information and communications technologies ("ICT") and financial business. However, some regulations from the Internet-Only Bank Act are found to be stricter than those of the Banking Act. For example, internet-only banks may only lend funds to a company that is a small or medium-sized enterprise, and to a person who is a large stockholder of such company.

- Payment and settlement service: the operation and management of the payment and settlement system is mainly based on the Bank of Korea Act and its sub-regulations, "Rules for the Operation and Management of Payment Systems". A payment service provider may provide services by participating in the "Payment and Settlement System," such as a large-scale payment system operated by the Bank of Korea, a small payment system operated by the Korean Financial Telecommunications & Clearings Institute ("KFTC"), etc. Payment service providers shall observe the Banking Act, FISCMA Act, SCFB Act, ETF Act, etc. applicable to its own types of payment and settlement service. In relation to payment and settlement services with non-cash and paperless payment methods, the SCFB Act contains a regulation for credit card businesses, and the ETF Act deals with electronic financial transactions with electronic payment means. The ETF Act defines "electronic payment means" as an electronic funds transfer, electronic debit payment means, electronic prepayment means, electronic currency, a credit card, an electronic bond or other means of payment by electronic means.

The ETF Act stipulates issuance and management of electronic payment means, permission and registration of electronic financial business, and measures ensuring the safety of electronic financial transactions and protection of users. Most fintech payment services are treated as "electronic payment settlement agency services", which are services that are rendered to transmit or receive payment settlement information in purchasing goods or using services by electronic means, or to execute as an agent or mediate the settlement of prices thereof. Also, most fintech remittance services are treated as "issuance and management of electronic prepayment means business", as prepayment means are used to remit funds between different bank accounts.

However, it is impossible for many fintech companies to directly participate in the payment and settlement system, because transactions using the electronic payment means under the ETF Act are executed through the accounts of financial companies, such as banks or a few securities firms. Moreover, a transfer of funds between deposit accounts can only be done by participating in the KFTC-operated payment system, which requires a membership with KFTC, a non-profit corporation, under the KFTC regulations. As it is difficult for fintech companies to directly participate in the

payment system, an open banking system is being promoted as an innovation. (*See* “Introducing open Application Programming Interface for open banking”.)

- Money-lending business: the SCFB Act and Act on Registration of Credit Business, etc. and Protection of Finance Users are applicable to credit loans or money-lending businesses without receipt of deposits, contrary to banks. Among the above, the SCFB Act deals with credit card business, facility-leasing business, installment-financing business, and new technology venture capital business. Meanwhile, the Act on Registration of Credit Business, etc. and Protection of Finance Users is composed of regulations on credit business and loan brokerage business. Also, the credit business mentioned in the Act on Registration of Credit Business, etc. and Protection of Finance Users is primarily a business that lends small amounts of money to low-credit consumers.

However, there are no specific laws to regulate the peer-to-peer (“P2P”) financing platform. A P2P lending business model can be interpreted as a credit business or loan brokerage business depending on the specific business model’s characteristics. A credit business or a loan brokerage business is required to register with the competent authority having jurisdiction over the business’ office, such as the Special Metropolitan City Mayor, Metropolitan City Mayor, etc. On the other hand, if the platform simply relays information between borrowers and lenders online and is not involved in the direct loan contract-making process, such platform may not be considered as a credit business or loan brokerage business. A P2P financing platform that is neither a credit business nor loan brokerage business is usually connected to “a credit business linked to online loan information” registered under the Act on Registration of Credit Business, etc. and Protection of Finance Users. Also, a credit business linked to online loan information must observe the “P2P loan guideline” of the FSC, which provides duties of public notice, unsound or high-risk business restrictions, security standards, and management of conflict.

Meanwhile, bills concerning the regulation of P2P financing are currently pending at the National Assembly as of June 2019.

- Financial investment service and asset management: the FISCMA Act includes regulations for financial investment instruments, such as securities and derivatives, and financial investment business that is classified as investment trading business, investment brokerage business, collective investment business, investment advisory business, discretionary investment business and trust business. Among the financial investment businesses, crowdfunding with issuance of securities is relevant to “investment brokerage business” under the FISCMA Act, where a “crowdfunding broker” is defined as an investment broker engaging in the online brokerage of public offering or sale of debt securities, equity securities and investment contract securities issued by a person who is within the requirements of the Presidential Decree and the Support for Small and Medium Enterprise Establishment Act, etc., on another person’s account in whosever named by the method prescribed by Presidential Decree. Meanwhile, personalised asset management and robotic adviser services with AI are related to “investment advisory business” or “discretionary investment business” that use electronic investment advisory devices under the FISCMA Act.
- Insurance: the Insurance Business Act is applicable to InsurTech as well as traditional insurance business. Any person who intends to be an insurance agency shall apply for registration with the FSC. However, an electronic financial business entity is not allowed to run an insurance agency except for a “specific product non-life insurance agency”, which is a non-life insurance agency that solicits insurance products relevant

to a person's business where such person's business mainly focuses on the sale of specific goods or the provision of specific services.

- Foreign exchange transactions: in order to engage in foreign exchange affairs such as payment, collection and receipt between the Republic of Korea and a foreign country, a company shall observe the Foreign Exchange Transactions Act. Pursuant to the Foreign Exchange Transactions Act, a financial company, etc., who is a financial company under the Act on the Establishment, etc. of the FSC and other relevant laws, may perform foreign exchange affairs by registering itself with the Minister of Strategy and Finance in advance, with its capital, facilities and professional human resources sufficient to perform such affairs. However, if a company that is not a financial company, etc. intends to engage in foreign exchange affairs, it may register its business by fulfilling easier requirements than a financial company, etc. and execute only a limited amount of transactions. In addition, in accordance with the ETF Act, companies that have been authorised or registered as businesses issuing and managing electronic currencies, electronic prepayment means or electronic payment settlement agency services can also register with the Minister of Strategy and Finance for other specialised foreign exchange business and provide payment services overseas.
- Financial data protection: the Credit Information Use and Protection Act stipulates principles and standards related to the use and protection of credit information, while the Personal Information Protection Act provides regulations for the processing and protection of personal information, and the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. deals with protecting personal information when using information and communications services. Regarding financial data protection, the Credit Information Use and Protection Act has priority, while the Personal Information Protection Act, the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc., the ETF Act and the Act on Real Name Financial Transactions and Confidentiality become applicable to any matters that are not provided in the Credit Information Use and Protection Act.
- Financial innovation support: on April 1, 2019, the Special Act on Financial Innovation Support was enacted with the purpose of promoting the development of innovative financial services. The Special Act on Financial Innovation Support is applicable in preference to other finance-related laws, such as the Banking Act, FISCM Act, SCFB Act, ETC Act, Credit Information Use and Protection Act, Personal Information Protection Act, Act on Promotion of Information and Communications Network Utilization and Information Protection, etc., and so forth. The Special Act on Financial Innovation Support provides the designation of innovative financial service by the FSC and support of innovative financial services, the responsibility of designated innovative financial service providers, and matters concerning designated agents who can be entrusted with the work of a financial company. Designated innovative financial services providers must inform the customer in advance that the service is in test operation and that unexpected risks may arise and, furthermore, obtain consent from its users about providing innovative financial services. Also, designated innovative financial services providers shall not only indemnify a customer against damages caused by the provision of services, but shall also be insured against liability for damages.

Meanwhile, Korea has incorporated the financial supervisory system as advised by international bodies.

- Korea joined the Financial Action Task Force on Money Laundering (“FATF”) in October 2009, and complies with their recommendations. In an effort to prevent money laundering, the Act on Reporting and Using Specified Financial Transaction Information includes the definition for money laundering, and criminalisation of money laundering is included in the Act on Regulation and Punishment of Criminal Proceeds Concealment and Act on Special Cases Concerning the Prevention of Illegal Trafficking in Narcotics, etc. Moreover, regarding cryptocurrencies, the FSC provides a cryptocurrency-related anti-money laundering guideline. In addition, Korea will receive a reciprocal evaluation on the operation of AML/CFT (Anti-Money Laundering/Countering the Financing of Terrorism) starting from January 2019 until February 2020, under the FATF Mandate.
- As the UN has adopted the International Convention for the Suppression of the Financing of Terrorism 1999, as a member of the UN, Korea also implemented the Act on Prohibition Against the Financing of Terrorism and Proliferation of Weapons of Mass Destruction in December 2008.
- As the Basel Committee on Banking Supervision (“BCBS”) enacted the “International Agreement on Self-Capital Measurements and Standards” in July 1988, Korea also introduced the concept of the equity ratio for risk-weighted assets as part of the management guidance standard for banks in 1992, and implemented the equity capital reserve system considering market risks in January 2002. As the BCBS announced the Basel III in December 2010, as a member of the Basel Committee, Korea also implemented the Basel III gradually from December 2013. Furthermore, the BIS-based equity capital ratio was also introduced in 1998 to mutual savings banks, and non-banking financial companies.

To address the new developments in the area of fintech, the following attempts are being made by government and financial authorities.

- Introducing the principle of technology neutrality in authentication: the ETF Act and sub-regulations were amended in March 2015 to abolish the obligation to use the authorised certificate, so that various authentication technologies could be used in electronic financial transactions. This amendment introduced the principle of technology neutrality according to which the law refuses to enforce the use of particular technologies or services, but promotes competition in certification technologies.
- Introducing the Virtual Test-Bed: the Virtual Test-Bed system was introduced to enable pre-testing of financial services in a virtual environment that is similar to the actual financial market. In August 2016, the KFTC established the world’s first joint fintech open platform (“Open API + Test bed”) at an open platform centre, which supports infrastructure and provides consulting for evaluating the normal operation of fintech services on a financial network. Also, the FSC implemented the Robo-Advisor Test Bed system in August 2016. Operation of the Test-Bed is carried out by Koscom, a company that builds and operates computer systems for the capital market, where its shareholders are composed of the Korea Exchange, the Korea Securities Depository, and 14 securities companies. The TestBed consists of a pre-examination, a main review and the deliberation of the final civilian review committee. The pre-examination verifies the specifications and algorithms of a company, and examines the capacity of the algorithm’s portfolio yielded by the investor’s inclination, based on hypothetical investor information. The main review requires actual funds to be operated for six months on a portfolio derived from the pre-examination, in order to

verify the stability of the algorithm and also to conduct a system review of security and stability. Passing the Test-Bed review allows the robo-advisor to conduct consultations or to operate customer assets directly without the involvement of professionals in the future, and it also allows the use of Test-Bed pass results and performance in the company's investment advertising.

- Introducing the Test-Bed system in connection with statute: in March 2017, the FSC announced measures to introduce a Test-Bed for financial regulation for an early settlement of innovative financial services. The Test-Bed system introduced by the FSC consists of the FSC's issuance of non-action opinions, test assignment programme through a financial company, and designated agent to which a financial company's business is entrusted. Among them, the issuance of non-action opinions and test assignment programme through a financial company were enforced without specific revisions to law, but the designated agent to which a financial company's business is entrusted was reflected in the Special Act on Financial Innovation Support, which took effect in April 2019.
- Establishment of Quick Response ("QR") Code Payment Standard: in November 2018, the FSC published the QR Code Payment Standard to ensure availability, simplicity and security of payment while issuing, using and destroying QR codes in electronic financial transactions. In particular, the QR Code Payment Standard ensures that the QR code has its own security functions to prevent any forgery or tampering, and also to prohibit the inclusion of sensitive personal or credit information.
- Convergence of the financial and non-financial sectors: the Internet-Only Banks Act amended the principles of segregation between bank capital and industrial capital. (See "Key fintech-related regulations" – Banking business.) Also, the Banking Act and Act on the Structural Improvement of the Financial Industry and Financial Holding Companies Act prohibit financial companies from possessing stock ownership in general, and the only exception would be when the two companies' businesses are related. Of course, the financial company should obtain the FSC's approval or report to the FSC prior to the acquisition of the non-financial company's stock, while the FSC clarified the types of fintech company businesses in which financial companies may invest by issuing an official opinion on the interpretation of the statute in May 2015, in order to stimulate investment in fintech companies. However, due to restrictions under the Insurance Business Act, an insurance company still cannot have a fintech company as a subsidiary.
- Introducing open Application Programming Interface ("API") for open banking: the financial authorities are introducing policies to transform the financial settlement infrastructure from a closed API, which allows access to programs only through APIs within the company or among pre-linked financial firms, to an open API. Through the open API on the financial settlement infrastructure, fintech firms that do not have membership in the existing financial company payment settlement network can also provide payment and remittance services and financial transaction information enquiry services using the open API. The government and the financial authorities are revising laws and encouraging existing financial companies to participate in open banking with open API. As a result, the Joint FinTech Open Platform was established in August 2016 and some payment and data enquiry functions from 16 banks were made available through open API. The FSC also announced in February 2019 that it would promote the open API in various financial industries in the long term, including securities and insurance, in addition to the banking sector.

- Activating the big data industry in the financial sector: the MyData business is in the process of making financial data which is stored in various financial institutions available to users. The revision of the Credit Information Use and Protection Act is pending at the National Assembly to make the use of MyData by customers and the disclosure of financial institutions legally mandatory. In addition, the FSC is introducing the Data Standards API in order to facilitate data retrieval and movement, and it is establishing a database of financial standard information that is open to public in the financial sector, such as DART electronic disclosure.
- Enactment of the Special Act on Financial Innovation Support: the Special Act on Financial Innovation Support was implemented in April 2019 to set an exception to several regulations related to banking, electronic finance and financial data protection, and to lay the legal basis for fintech support policies. Based on the Special Act on Financial Innovation Support, the FSC may designate a fintech service with high innovation and consumer benefits as innovative financial services considering the opinion of the Innovation Financial Review Board and grant necessary regulatory exceptions for market testing, to a limited extent. In addition, the Special Act on Financial Innovation Support provides an incentive for a company designated as an innovative financial service to explore new business opportunities by ensuring such company the exclusive operation rights for the innovative financial service for two years, provided the company obtains the relevant licence for the financial business.

Restrictions

In common law countries adopting a principle-based legal system, a financial supervisory service typically has the power to determine the applicability of specific regulations and licensing requirements at its discretion. However, in Korea, there is only limited room for discretion on the part of the financial regulator in determining the requirements and imposition of financial regulations, due to a regulation-oriented legal system and with individual financial business laws. Accordingly, an opinion of a financial regulator is often not anticipated for a legitimate start of a new project as it is not provided by the existing individual financial business law. The National Assembly or the government should revise the individual financial business laws and their sub-regulations.

Also, the establishment of a financial company requires approval from the FSC or registration with the FSC. When the FSC approves the establishment of a financial institution, the FSC not only conducts a Fit and Proper Test for management and majority, but also requires the quantitative requirements set out in the Act for Safe Management of Financial Institutions to be met. For instance, the Banking Act requires large shareholders to have sufficient investment capacity, sound financial position, and social credit.

On the other hand, the Special Act on Financial Innovation Support introduced strong incentives for fintech companies. Businesses designated as innovative financial services enjoy exemptions from various legal restrictions for a certain duration. Furthermore, if a fintech company, designated as an innovative financial service, acquires a licence with the conditions required by the relevant financial law, an exclusive right is guaranteed to such company by prohibiting other companies from providing the same service to the market for two years after entering the market in earnest.

Also, the FinTech Support Center was opened in March 2015 as a department dedicated to the creation of fintech ecosystems. In addition, in order to reduce risks to new businesses without waiting for the revision of the current laws and sub-regulations, the FSC issued non-

actional advice, and the Special Act on Financial Innovation Support introduced a prompt regulatory confirmation system.

Cross-border business

Strict regulations on the finance industry in Korea have been barring foreign fintech companies from entering the Korean market. As Korean government began to amend or lighten such regulation to encourage the fintech industry, the Korean market opened the door to foreign fintech companies. TransferWise is one of the foreign fintech frontiers to enter the Korean market. As the Foreign Exchange Transaction Act was amended to allow stock, insurance, and fintech companies to carry foreign overseas remittance of small sums, TransferWise partnered with the local company PayGates to launch a beta service for inbound remittances in December 2018. Because TransferWise does not rely on licensed banks and exchange currencies by matching or pairing people with the target currency directly, the exchange process and fee are reduced greatly. It is expected that other global fintech companies will increasingly begin business in Korea, and local and traditional financial companies will need to keep up with the trend and develop fintech technology to survive.

It is not only companies which need to change. To follow the trend, the FSC has been regularly holding the International Financial Cooperation Forum since 2013 to share concerns on financial matters and develop networks between Korean and overseas financial institutions. High-level officials from foreign financial authorities including Bangladesh, Cambodia, China, Indonesia, Laos, Myanmar, Singapore, Vietnam and other ASEAN countries and officials from international organisations including the IMF, World Bank, and UN ESCAP (Economic and Social Commission for Asia and the Pacific) attended the forum to discuss financial issues in the Middle East, Northern Africa and Southeast Asia.

Further, the FSC formed a fintech bridge by signing a regulatory co-operation agreement on sharing information in relation to fintech innovations with the UK's Financial Conduct Authority in July 2016. Under the fintech bridge, Korea received advice on how to devise and operate a sandbox more efficiently and shared experience on cryptocurrency regulations. Korea and the UK upgraded the agreement in June 2018 by agreeing that each financial authority will support a fintech company who wishes to enter into its market if the other financial authority gives referral.

In relation to the supervision and investigation of the fintech industry, the chairman of the FSS emphasised the necessity and importance of cooperation between financial authorities in each country in fintech crimes and unethical actions in September 2018, because fintech technologies, for example, cryptocurrency, have global impact; independent regulation by the respective country will only benefit wrongdoers. Such cooperation is yet to be made, but it not an unrealistic daydream, as the FSC and FSS were approved by the International Organization of Securities Commissions as the tenth regular member of the Enhanced Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information (the "EMMoU") on December 2018. The EMMoU is an agreement between financial authorities to cooperate in investigations and prosecutions on unfair trade by sharing audit work papers or financial statements, freezing assets and more.

**Won H. Cho****Tel: +82 2 2051 1870 / Email: whc@dlightlaw.com**

As an experienced patent lawyer with extensive commercial transactional experience in various specialty industries including entertainment, ICT and healthcare, Won H. Cho is uniquely positioned to advise clients on a wide range of complex IP, corporate and regulatory matters. He started his career as an associate at Bae, Kim & Lee LLC (“BKL”) and went on to serve as a partner of the firm, leading BKL’s prominent IP and technology transaction practices, spanning a total of 16 years. Mr. Cho also worked on secondment at Ropes & Gray (New York) in 2014 in the firm’s IP division. Recently, he has been actively advising clients in the blockchain industry.

Mr. Cho is now an adjunct professor at KAIST-MIP (Master of Intellectual Property) and serves in leadership roles at various local and state organisations, including the Korea Fair Trade Commission Advisory Committee, Korean Intellectual Property Office, US Korea Law Foundation, Korea Licensing Executive Society, and the Korea Association of Entertainment Law, among others. Mr. Cho holds a B.A. from Seoul National University and received an LL.M. from the University of Texas.

**Hye In Lee****Tel: +82 2 2051 1870 / Email: hil@dlightlaw.com**

Hye In Lee is an associate at D’LIGHT, where she focuses on advising and assisting in litigation and legal issues in the ICT and fintech industries, including blockchain systems. Ms. Lee also has extensive field experience in both international legal cases, such as global investment, M&A and international arbitrations, and local legal cases, including IP litigation, financing, investigation by the public prosecutor and/or the Korean Free Trade Commission, from her time as corporate counsel at Samsung C&T Corporation and Netmarble Corporation.

**Hyeseon Han****Tel: +82 2 2051 1870 / Email: hsh@dlightlaw.com**

Hyeseon Han is an associate at D’LIGHT, where she focuses on advising and assisting in litigation and legal issues in the fintech industries and foreign exchange regulations. Ms. Han studied economics at Seoul National University before accumulating practical experience in international trade and transportation at a global shipping company and acquiring a licence as an International Trade Specialist. Based on her understanding of the financial sector and as a certified Fund Investment Solicitor, Ms. Han counsels clients on financial regulation, fintech, corporate finance and PEF. Ms. Han also has extensive experience in corporate civil and administrative litigation cases.

D’LIGHT Law Group

8th Floor, 311, Gangnam-daero, Seocho-gu 06628, Seoul, Korea
Tel: +82 2 2051 1870 / URL: www.dlightlaw.com

Luxembourg

Prof. Jean-Louis Schiltz & Nadia Manzari
Schiltz & Schiltz S.A.

Approaches and developments

Luxembourg has always considered innovation as an essential driver for the development of financial services and the financial sector in general. In 2014, the Luxembourg Government launched its Digital Luxembourg initiative of which Fintech is a key component, the aim being to bring finance to the 21st century. The Luxembourg mindset which consists of embracing and fostering change has contributed to the creation of a very successful and dynamic financial technology (“Fintech”) sector in Luxembourg. A growing number of companies from around the world are opening offices in Luxembourg to develop and market their product range in Europe and worldwide.

Fintech has been around for a long time in Luxembourg, even before the concept became known as such. The fund industry has indeed been using Fintech solutions for many years (Multifonds is one of the historic examples). Luxembourg has generally been very active in digital innovation and was amongst the first countries in Europe to implement the European payment services directive¹ in 2009. This “first mover” advantage in particular enabled the country to develop a strong track record in payments services, and this led in turn to the creation of an ecosystem of highly innovative products.

Luxembourg’s financial centre provides an attractive environment for Fintech companies. The presence of 146 banks,² the world’s leading funds industry, a good developed insurance and reinsurance sector and financial infrastructures like central securities depositories provide for a large potential client base.

Excellence in the field of IT in particular gives Luxembourg a competitive advantage over other countries thanks to the presence of the largest number of Tier IV data centres in the world, guaranteeing data availability and security at the highest standards.

The country is also intensely working on blockchain technology. The creation of the Infrachain initiative, which combines the transparency of public chains with the flexibility of private chains, is one of the flagship examples in this context. It aims at enabling companies to customise blockchains for specific needs. In the same vein, the Luxembourg University, through its Center for Security Reliability and Trust, is at the forefront of the research activities based on or related to distributed ledger technologies. It has, for instance, just recently announced a partnership with US-based Ripple.³ Most importantly, the country has recently adopted a law setting out “black and white” that securities can be legally held and transferred through distributed ledger technologies,⁴ thus adding one more layer to its long tradition of “innovation through law”, of which legal certainty is one of the essential pillars.

Fintech offering in Luxembourg

Luxembourg has a diversified Fintech ecosystem composed of Fintech firms, finance-related software vendors as well as IT solution providers. More than 40 of them are, for instance, active in the payments sector, offering innovative digitised payment solutions to consumers as well as to merchants.⁵

To name just a few examples, PayPal (Europe) S.à r.l. et Cie, S.C.A. was granted a banking licence in Luxembourg in 2007. Amazon Payments Europe S.C.A has had an e-money licence in the Grand-Duchy since 2010 and in 2016, Rakuten Europe Bank S.A., after having initially obtained a payment licence, obtained a banking licence. PingPong was one of the first Chinese Fintechs to obtain a European payment licence in Luxembourg back in 2017. Bitstamp was the first crypto-exchange to become licensed as a payment institution in Luxembourg in 2016, the Luxembourg regulator thus obliging for the first time in Europe crypto-clients to abide by AML/CTF requirements (Europe has followed the same path in the meantime). Ebay S.à.r.l is also operating its payment services in Europe under a payment institution licence granted by the Luxembourg Ministry of Finance in 2014, and Payconiq International S.A. has recently been acquiring Digicash – a booming Luxembourg mobile payments company – in order to establish a Benelux-wide presence of its mobile payments initiative. Recent press reports also indicate that Airbnb is in the course of applying for a licence in Luxembourg.

A large number of Fintech companies in Luxembourg are active in the fund – and the investment industry at large – as well as in the banking and insurance sectors. Fintech companies in Luxembourg are also omnipresent in the fields of big data, artificial intelligence (“AI”), cybersecurity, authentication (KYC), cryptocurrencies and blockchain.⁶

Over the last five years, local and international banks, professionals of the financial sector and insurance companies have deployed impressive energy and expertise in Fintech, regulatory technology (“Regtech”) and insurance technology (“Insurtech”). Across the different industries, we are seeing more and more M&A activity and collaboration at large between Fintechs and traditional actors, with the result that these traditional actors rapidly achieve innovative new offerings.

In line with the concept of “innovation through law”, Luxembourg in the first place always aims to apply existing laws and regulations to new models. A striking example is the application of the payment legislation to crypto-exchanges (whereas, in contrast, other countries decided not to regulate this type of activity, leaving the actors established in their territory in a grey area, to say the least). Only where existing legislation is not clear enough, or where existing legislation is totally silent about a certain type of activity, does Luxembourg enact new legislation. The most striking example here is the new law of 1 March 2019⁷ on transfers of securities via distributed ledger technologies.

Regulatory and insurance technology

As part of the booming Fintech sector, an impressive number of Regtech providers have grown out of Luxembourg over the last years. Among the most well-known actors, Governance.com, Seqvoia, KYC TECH, FINOLOGEE or LUXHUB, each in their own field, for instance assist financial institutions to face ever increasing regulatory requirements. Regtech companies in Luxembourg mainly provide services based on automated processes in the areas of anti-money laundering (KYC), reporting and risk management, thus enabling better and more efficient risk identification and regulatory compliance.

The adoption of Insurtech solutions is going smoothly in Luxembourg. Tools are becoming increasingly sophisticated and innovative. Claims handling and actuarial calculations are just two examples of areas of predilection for their implementation.

Looking at Insurtech from a wide angle, it can be observed that Luxembourg's insurers are at the forefront of innovation when it comes to driverless or so-called autonomous cars. The Association of the Luxembourg Insurance Companies, together with the University of Luxembourg and Schiltz & Schiltz S.A., has indeed recently organised a mock trial about a fictitious car accident that "took place" in 2030, and in which a driverless car hit a pedestrian. The case was pleaded in front of real judges in the Court house of Luxembourg City, and the judges handed down a real fictitious judgment. In this judgment, the Court held that the ancient theory distinguishing between the structural custody and behavioral custody of an object (here: the vehicle) was as a matter of principle relevant for assessing liability claims in the context of driverless cars. It also held that for the car maker, the law on civil liability for defective products needed to be analysed. In the end (and in short), the driver was held liable because it was established that he did not follow the voice instructions of the car.

Regulatory bodies

Fintech entities established in Luxembourg and that are subject to regulatory supervision (many are not) are supervised by the Luxembourg supervisory authorities. Depending on their licence, they may fall under the supervision of the *Commission de Surveillance du Secteur Financier* ("CSSF") or the *Commissariat aux assurances* ("CAA"). The Central Bank of Luxembourg ("BCL") has competences, amongst others, with regard to the security of payment systems and payment instruments and the *Commission Nationale pour la Protection des Données* ("CNPD") is the authority in charge of data protection.

*The CSSF is a public institution which supervises the professionals and products of the Luxembourg financial sector. It supervises, regulates, authorises, informs, and, where appropriate, carries out on-site inspections and issues sanctions. Moreover, it is in charge of promoting transparency, simplicity and fairness in the markets of financial products and services and is responsible for the enforcement of laws on financial consumer protection and on the fight against money laundering and terrorist financing.*⁸

*The CSSF performs its duties of prudential supervision and supervision of the markets for the purposes of ensuring the safety and soundness of the financial sector, solely in the public interest.*⁹

The Central Bank of Luxembourg has within its tasks to ensure the efficiency and safety of payment systems as well as the safety of payment instruments. The means of coordination and cooperation employed for the performance of these tasks are subject to agreements between the BCL and the CSSF, complying with the legal competences of the parties.¹⁰ For the purpose of performing its tasks related to the safety of payment instruments, the BCL may ask issuers of payment instruments to provide any information relating to those payment instruments which is necessary in order to assess their safety. Additionally, the BCL is authorised to undertake on-site visits in order to collect the information and coordinates with the CSSF to this end.¹¹

*The CAA is the competent supervisory authority for the insurance sector in Luxembourg, which includes the insurance companies, reinsurance companies, certain pension funds, the professionals of the insurance sector (PSA) and insurance and reinsurance intermediaries (agents and brokers).*¹²

*The main objective assigned to the CAA is to ensure the protection of the insurance takers and the beneficiaries. This objective includes the examination of the applications for approval of natural and legal persons under the supervision of the CAA, the prudential supervision of the same natural and legal persons and the supervision of the market in insurance products. The CAA is also competent for monitoring compliance with professional obligations in the fight against money laundering and terrorist financing in the insurance sector.*¹³

*The CNPD verifies the legality of the processing of personal data and ensures the respect of personal freedoms and fundamental rights with regard to data protection and privacy. Its mission also extends to ensuring the respect of the amended Act of 30 May 2005 regarding the specific rules for the protection of privacy in the sector of electronic communications.*¹⁴

Key regulations and regulatory approaches

Key regulations

In line with the principle consisting of “applying existing laws and regulations to new models”, the Luxembourg legislator (Parliament) has not so far enacted numerous Fintech laws. There is indeed only one example of a new specific Fintech law that has been enacted by Parliament up to now, and that is the above-mentioned law of 1 March 2019 amending the law of 1 August 2001 concerning the circulation of securities, which aims at promoting the use of distributed ledger technologies for the circulation of securities by setting out, “black and white”, that securities can be legally transferred through distributed ledger technologies, including blockchain. Whilst it can for sure be argued that securities could be held on the blockchain even before the enactment of the new law, article 18*bis* – which is the new article added to the law of 1 August 2001 – provides the financial sector with crystal-clear legal certainty, thus enabling the various actors to fully take advantage of the opportunities offered by distributed ledger technologies in the field of securities.

For the rest, and in addition to this one and only example when Parliament enacted a specific Fintech law, Fintech actors and activities fall under the scope of existing laws and regulations, with the CSSF issuing specific secondary legislation through circulars or general guidance in a number of areas.

Whilst historically, Fintech activities developed first in the payments industry, it nowadays impacts the entire financial industry, from banks to start-ups as well as investment services and the fund industry. Clearing and settlement infrastructures as well as the Luxembourg Stock exchange are equally running Fintech projects today.

Fintech companies, whilst building the services they offer on innovative technologies, often provide financial services and in that case they do fall – just like traditional companies providing financial services – into the scope of the CSSF’s supervisory competences (and whether or not a certain law or regulation then applies to such services depends on the Fintech product or service offering). For example, Fintech payment products – such as the use of digital payment methods which are intended to be used as a means of payment for acquiring goods or services or as a means of money or value transfer – will be subject to the modified Law of 10 November 2009 on payment services, on the activity of electronic money institution and settlement finality in payment and securities settlement systems (“Law of 10 November 2009 on payment services”).

An example of regulatory guidance issued by the CSSF is the area of robo-advisory. According to the CSSF, investment services based on robo-advisory tools do fall under the

remit of the Law of 5 April 1993 on the financial sector, as amended (“Law of 5 April 1993 on the financial sector”). In a position paper on robo-advice published on 27 March 2018,¹⁵ the CSSF outlined that the type of licensing required by a robo-advisor to perform its activities depends on the operating model chosen, including the services provided, the contractual arrangements and the structure of the platform. Therefore, robo-advisors need to register as investment advisers¹⁶ – just like traditional, non-automated financial advisers – when they merely provide advisory services without intervening in the implementation of the advice they have provided. The CSSF paper also considers that whenever robo-advisors use robo-technology to manage portfolios as per clients’ mandates on a discretionary client-by-client basis, they need to register as private portfolio managers.¹⁷ Furthermore, the CSSF considers that robo-advisors need to register as brokers in financial instruments¹⁸ when their servicing consists of that of an intermediary by either encouraging parties to be brought together with a view to conclude a transaction, or by passing on their clients’ purchase or sale orders without holding the investments of the latter. Finally, in cases where a robo-advisor executes orders on behalf of clients in relation to one or more financial instruments, the robo-advisor needs to apply for an authorisation as a commission agent.¹⁹ The paper specifies that in any of the above-mentioned cases, robo-advisors have to comply with the MiFID/MiFIR framework.

For tokens – which continue to be a hot topic in Luxembourg – the general position in Luxembourg is that asset tokens, which represent a debt or equity claim on the issuer, entitling, for example, the holder of a share in future company earnings or future capital flows (which could, in terms of their economic function, be compared to equities, bonds or derivatives), or tokens which enable physical assets to be traded on the blockchain, would fall under the remit of different regulatory frameworks, depending on the exact qualification of the token and on the financial service provided. As a consequence, the following laws may apply:²⁰

- Law of 10 July 2005 on prospectuses for securities;
- Law of 5 April 1993 on the financial sector;
- Law of 30 May 2018 on markets in financial instruments;
- Law of 17 December 2010 relating to undertakings for collective investment; and
- Law of 12 July 2013 on alternative investment fund managers.²¹

Regtech companies providing services and solutions in order to assist financial actors to comply with regulatory requirements can also be subject to regulatory supervision. Depending on their set-up and the services they provide, a licence as a support professional of the financial sector (“support PFS”) as per the Law of 5 April 1993 on the financial sector may be required for a number of these companies, whereas for others, i.e. those merely providing technological solutions (software in the wider sense), no specific licence would be required. The support PFS licence is a Luxembourg-specific licence aiming at including in the supervision of the financial sector a certain number of activities that are connected to or closely interlinked with a financial activity. Licensing as a client communication agent,²² administrative agent of the financial sector,²³ primary IT system operator,²⁴ secondary IT systems and communication networks operators²⁵ may therefore have to be considered by Regtech firms.

In this context, two Regtech entities have been granted a licence in the first quarter of 2019: FINOLOGEE, which has been authorised as a client communication agent and a secondary IT systems and communication networks operator; and LUXHUB, which has been granted a licence as a secondary IT systems and communication networks operator.

In the insurance sector, no new Insurtech-specific regulations have been issued by the CAA so far.

It has to be noted that every regulated Fintech or Insurtech product or service also falls under the remit of the Law of 12 November 2004 on the fight against money laundering and terrorist financing.

Finally, it goes without saying that Luxembourg Fintech/Regtech/Insurtech companies have to comply with the European Union General Data Protection Regulation (“GDPR”), which imposes rigorous requirements on the controlling and processing of personal data. In this context, it must, *inter alia*, be ensured that only relevant and accurate personal data are processed and that the reinforced and partially new rights of data subjects are being complied with.

Regulatory approaches

The CSSF is on record for establishing a constructive and open dialogue with the Fintech industry by making itself available for all entities wishing to present an innovative project. In this context, the CSSF provides entities with advice and guidelines on the applicable regulatory framework in order to ensure that the project is developed in compliance with the regulations in force. In order to remain reactive, the CSSF is open to consultation regarding the future development of the legislation, given the market’s expectation, by enhancing the communication with market players. The CSSF thus offers itself a means to ensure appropriate information from market players regarding regulation, whilst remaining immersed in market evolution in order to anticipate challenges.²⁶

Regarding cloud computing, the Luxembourg financial supervisor has issued a pro-cloud position on 17 May 2017 by publishing Circular CSSF 17/654, which is supported by technical guidelines related to the use of some specific cloud products. It has also published on its website frequently asked questions on cloud computing.²⁷ Circular CSSF 19/717 was published on 27 March 2019, updating Circular CSSF 17/654, with the objective to apply more proportionality to the treatment of the notification process for non-material outsourcing to cloud computing infrastructures, as the initial circular revealed itself to be too burdensome in certain instances both for supervised entities and for the CSSF.²⁸

On 8 March 2018, the CSSF also published updated frequently asked questions on AML/CTF and IT requirements for specific customer on-boarding/KYC methods for identification/verification through video chat.²⁹

With regard to robo-advice and as detailed above, the CSSF published on 27 March 2018 a position paper outlining the licence requirements for robo-advisors.

In the context of artificial intelligence, the CSSF has carried out a research study in order to better understand AI. The result of the research, which has been made public, aims at spreading basic knowledge about AI, describing the different types of AI together with practical use cases for and in the financial sector. Furthermore, the study covers the analysis of the main risks associated with AI technology and provides some key recommendations to take into account when implementing AI into a business process.³⁰

As for Insurtech, even though – as indicated above – no new specific Insurtech regulations have been issued so far, it is by no means anticipated that the CAA will want to put barriers in place for Insurtech solutions – in fact, the opposite is true.

Influence of supra-national regulatory bodies

The CSSF does closely cooperate with supra-national regulatory bodies such as the European Banking authority (“EBA”), the European Securities and Markets Supervisor (“ESMA”),

the International Organization of Securities Commissions (“IOSCO”), the Single Supervisory Mechanism (“SSM”), the European Insurance and Occupational Pensions Authority (“EIOPA”), the Committee of European Auditing Oversight Bodies (“CEAOB”), the Basel Committee on Banking Supervision (“BCBS”) and the International Monetary Fund (“IMF”). The CSSF is also closely involved with several international working groups dealing with AML/CFT issues, notably the Financial Action Task Force (“FATF”), the Joint Committee’s Sub-Committee on Anti-Money Laundering (“AMLC”) under the Joint Committee of the European Supervisory Authorities, the Expert Group on Money Laundering and Terrorist Financing (“EGMLTF”) of the European Commission and the Anti-Money Laundering Expert Group (“AMLEG”) of the Basel Committee on Banking Supervision.³¹

The CAA is a member of the European Insurance and Occupational Pensions Authority (“EIOPA”), the International Association of Insurance Supervisors (“IAIS”). The CAA is involved in the Expert Group on Banking, Payments and Insurance (“EGBPI”) as well as of the European Commission’s working groups, the FATF and the OECD.

The BCL is an integral part of the European System of Central Banks (“ESCB”).

The CNPD is a member of the European Data Protection Board (“EDPB”), the International Working Group on Data Protection in Telecommunications, the VIS Supervision Coordination Group (“VIS SCG”), the Europol Joint Supervisory Authority (“JSA”), the SIS II Supervision Coordination Group (“SIS II SCG”) and the Joint Supervisory Authority (“JSA”) for customs. In addition, the CNPD represents the Grand Duchy of Luxembourg in various Council of Europe committees.

Fintech platform and working-groups

One of the main Fintech regulatory working groups today is the Tech law group which is working under the auspices of the *Haut Comité de la Place Financière* (“HCPF”).

In 2008, the Luxembourg Financial Industry Federation (“PROFIL”) and the Luxembourg Government founded Luxembourg for Finance (“LFF”), an agency for the development of the Financial Centre. The objective of this public-private partnership is to develop Luxembourg’s financial services industry and identify new business opportunities. LFF, among others, monitors global trends in finance and provides informational material on products and services available in Luxembourg. It does so in particular in the Fintech area.

Luxembourg has furthermore created in 2016 a dedicated national Fintech platform, the Luxembourg House of Financial Technology (“LHoFT”).³² The LHoFT is a platform in charge of building and developing the growing national Fintech ecosystem. It should enable financial institutions, Fintech innovators, research, academia and public authorities to interact and develop solutions and products in order to cover specific industry needs.³³ The LHoFT also interacts with other Fintech hubs around the world encouraging domestic and international collaborations, working groups and initiatives.³⁴

The Luxembourg Bankers’ Association (“ABBL”) as well as the Association of the Luxembourg fund industry (“ALFI”) have also set up dedicated working groups in order to allow their members to engage with the Fintech community.³⁵

The ABBL’s Digital Banking and Fintech Innovation Cluster (“DBFI”) facilitates cooperation between banks and Fintech firms in Luxembourg and strives for supporting its members in embracing disruptive technologies to satisfy expectations of more and more demanding customers.³⁶

The University of Luxembourg is also heavily involved in many Fintech initiatives.³⁷

Restrictions

There are as such in Luxembourg no patent restrictions to the development of Fintech, Regtech or Insurtech activities. It accordingly will suffice to outline below a few aspects to be taken into account or to be borne in mind for Fintech activities:

No one shall be authorised to carry out a financial activity without a licence in Luxembourg or out of Luxembourg. This does not mean that every Fintech needs a licence, but every Fintech carrying out a regulated activity – in general, providing financial services – does. A Fintech company which would like to establish itself in Luxembourg shall accordingly define its business purpose and its activity in a sufficiently concrete and precise manner, so as to allow the CSSF to determine whether a licence and, if so, which licence is required; mere technology providers will, for instance, not be required to apply for and obtain a licence.

On virtual currencies, the CSSF has stated that: *“there is currently no legal framework in Luxembourg or at European level that specifically applies to virtual currencies. However, the CSSF reminds that it should be borne in mind that any provision of financial sector services by a natural or legal person requires an authorisation by the Minister of Finance. The CSSF furthermore clarifies that legal qualification of virtual currencies and services provided relating to these virtual currencies is complex, notably given the technical specificities inherent in the different types of virtual currencies. Therefore, the CSSF invites the persons that envisage exercising an activity associated with virtual currencies (such as the issuing of means of payment in the form of virtual or other currencies, the offer of payment services using virtual currencies or other, or the provision of virtual currency exchange services) to submit their draft documentation to the CSSF beforehand. The CSSF will then determine whether or not the activity is a regulated activity.”*³⁸ This statement is also to be viewed against the background of the payment licence issued to Bitstamp as a crypto-exchange.

On initial coin offerings (“ICO”) and tokens, the CSSF has informed service providers and initiators of ICOs that: *“– despite the lack of specific regulations that applies to ICOs – the activities related thereto or implied through the creation of tokens as for example the collection and raising of funds may – depending on their characteristics – be subject to certain legal provisions in Luxembourg and thus to certain supervisory requirements. The CSSF therefore explains that it will not hesitate to assess such fundraising activities by extending its analysis to the objectives pursued in order to assess whether it could be a scheme to circumvent or avoid financial sector regulations, notably the provisions of the amended Law of 10 July 2005 on prospectuses for securities and the Law of 5 April 1993 on the financial sector. In this context, the CSSF considers that for any fundraising, the initiators of such ICOs are required to establish anti-money laundering and terrorist financing procedures.”*³⁹

The common denominator here is that while being open to innovation, the CSSF is likely to regulate Fintech activities in a large number of instances and will not tolerate financial activities being undertaken out of Luxembourg without a licence.

In the insurance sector, legal issues, if any, generally do not arise under insurance sector regulations themselves, but more likely in a data protection environment. It will suffice to mention two examples here:

Processing health data can be a challenge against the background of the General Data Protection Regulation, which does not provide for a carve out or specific rules regarding the insurance sector, in particular life insurance.

New car insurance models include the tracking of the behaviour of the driver of a car through a dedicated app. Data protection can be a challenge here as well, in particular when it comes to the processing of data, the amalgamation of which may for instance show that a criminal offence has been committed (no matter whether such offence is a major one or not). There is at least one known example where this type of application has been debated in Luxembourg with the data protection authority.

Cross-border business

Luxembourg is the European centre from where Fintech companies can – in a regulated way – provide their services and develop their activities all over the European Union and in third countries. Since the European regulatory framework applies to most of the authorised Fintech activities, the providers that have obtained a licence can easily passport their services throughout the European Union.

Fintech has – more than ever – a very strong international and global dimension⁴⁰ which requires a common and harmonised response from the regulators of the financial sector and the insurance sector. In this context and as previously mentioned, the CSSF, the CAA, the BCL and the CNPD actively participate in all major supra-national regulatory bodies and working groups, thus continuing, together with others, to be at the forefront of innovation and contributing to shape the international regulatory landscape of Fintech, Regtech and Insurtech.

* * *

Endnotes

1. Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services.
2. Situation as per 16 April 2019.
3. <https://coinreport.net/university-of-luxembourg-ripple-initiative/>.
4. Law of 1 March 2019 amending the law of 1 August 2001 concerning the circulation of securities.
5. <https://www.Fintechmap.lu/>.
6. <https://www.lhoft.com/en/insights/the-luxembourg-Fintech-map>.
7. See endnote 4.
8. <http://www.cssf.lu/en/about-the-cssf/about-the-cssf/>.
9. <http://www.cssf.lu/en/about-the-cssf/mission-and-competences/>.
10. Article 2 (5) of the Law of 23 December 1998 concerning the monetary status and the Central Bank of Luxembourg.
11. Article 27-3 of the Law of 23 December 1998 concerning the monetary status and the Central Bank of Luxembourg.
12. <http://www.caa.lu/fr/le-caa> (non-official translation).
13. *Ibidem*.
14. <https://cnpd.public.lu/en/commission-nationale.html>.
15. http://www.cssf.lu/fileadmin/files/PSF/Robo_advice_270318.pdf.

16. Article 24 of the Law of 5 April 1993 on the financial sector.
17. Article 24-3 of the Law of 5 April 1993 on the financial sector.
18. Article 24-1 of the Law of 5 April 1993 on the financial sector.
19. Article 24-2 of the Law of 5 April 1993 on the financial sector.
20. *The Virtual Currency Regulation Review Luxembourg Chapter* by Jean-Louis Schiltz and Nadia Manzari.
21. *Ibidem*.
22. Article 29-1 of the Law of 5 April 1993 on the financial sector.
23. Article 29-2 of the Law of 5 April 1993 on the financial sector.
24. Article 29-3 of the Law of 5 April 1993 on the financial sector.
25. Article 29-3 of the Law of 5 April 1993 on the financial sector.
26. http://www.cssf.lu/fileadmin/files/Publications/Rapports_annuels/Rapport_2017/RA_2017_eng.pdf.
27. http://www.cssf.lu/fileadmin/files/Systemes_d_informations/FAQ_Cloud_Computing_Circular_17052017.pdf.
28. http://www.cssf.lu/fileadmin/files/Lois_reglements/Circulaires/Hors_blanchiment_terrorisme/cssf19_714eng.pdf.
29. http://www.cssf.lu/fileadmin/files/LBC_FT/FAQ_LBCFT_VIDEO_IDENTIFICATION_080318.pdf.
30. http://www.cssf.lu/fileadmin/files/Publications/Rapports_ponctuels/CSSF_White_Paper_Artificial_Intelligence_201218.pdf.
31. http://www.cssf.lu/fileadmin/files/Publications/Rapports_annuels/Rapport_2017/RA_2017_eng.pdf.
32. <https://www.luxembourgforfinance.com/en/financial-centre/fin-tech/>.
33. *Ibidem*.
34. *Ibidem*.
35. *Ibidem*.
36. <https://www.abbl.lu/abbl-clusters/dbfi/>.
37. For a recent example, see: <https://coinreport.net/university-of-luxembourg-ripple-initiative/>.
38. http://www.cssf.lu/fileadmin/files/Protection_consommateurs/Avertissements/W_virtual_currencies_140318_eng.pdf, 14 March 2018.
39. http://www.cssf.lu/fileadmin/files/Protection_consommateurs/Avertissements/W_ICOS_140318_eng.pdf, 14 March 2018.
40. On 4 October 2018, the CSSF has for instance signed a Cooperation Agreement with the Australian Securities & Investments Commission (“ASIC”), providing a framework for cooperation to understand financial innovation in each jurisdiction and for information sharing between the two regulators on Fintech and Regtech (http://www.cssf.lu/fileadmin/files/Publications/Communiqués/Communiqués_2018/P_R1832_ASIC_CSSF_Cooperation_Agreement.pdf).

**Prof. Jean-Louis Schiltz****Tel: +352 45 64 80 / Email: claudia.gierl@schiltz.lu**

Jean-Louis Schiltz is the Senior partner at Schiltz & Schiltz and Professor (hon.) at the University of Luxembourg.

Jean-Louis Schiltz is a regular speaker at tech law and innovation conferences and has authored and co-authored a number of articles and reports in the field over the last years. He serves as a member for a number of companies and non-profit organisations.

From 2004 to 2009, Jean-Louis served as Cabinet Minister in Luxembourg. His portfolio included media, telecommunications, technology, international development and defence.

Jean-Louis joined the firm in 1989 and was admitted to the Luxembourg Bar the same year.

Jean-Louis Schiltz holds a postgraduate degree (DEA) in business law from the University of Paris I, Panthéon-Sorbonne. He taught at his *alma mater* in the early 1990s.

**Nadia Manzari****Tel: +352 45 64 80 / Email: nadia.manzari@schiltz.lu**

Before joining the firm in 2018, Nadia was the Head of the Innovation, Payments, Markets Infrastructures and Governance Department at the *Commission de Surveillance du Secteur Financier* (“CSSF”), where she started her career in 2001.

She is a regular speaker at national and international conferences covering payment services, financial technologies, remuneration policies and corporate governance.

She graduated in law from the University Robert Schuman in Strasbourg and holds a Master’s degree in private law (*maîtrise en droit privé, mention “droit des affaires”*) as well as a postgraduate DJCE diploma (*Diplôme de Juriste Conseil d’Entreprise*) degree with a focus on German-French business law. She holds the Certificate in Corporate Governance of INSEAD and is an ILA certified director.

Schiltz & Schiltz S.A.

24–26, avenue de la Gare L-1610 Luxembourg
Tel: +352 45 64 80 / URL: www.schiltz.lu

Malta

Dr. Karl Sammut & Dr. Bradley Gatt
sammut.legal

Approaches and developments

Digital innovation is disrupting every industry and sector, and is presenting challenges and competition to the traditional financial services industry. Traditional financial services firms are facing challenges to the manner in which they conduct their businesses, particularly as regards the efficiency and cost-effectiveness of their operations which FinTech, on the other hand, seems to increasingly improve and overcome. FinTech combines traditional concepts in financial services with innovative and bespoke technologies that are set to revamp the financial services industry. In order to remain competitive, traditional financial services players have no choice but to remain relevant and up to date with new technologies.

Faced with concerns relating to certain risks and threats that FinTech may present to the financial services industry, particularly in relation to customer protection, the duty of any regulator is to ensure that such risks and threats are mitigated through robust regulation which regulates and protects both the service provider and the customer. In light of such challenges, any regulator should strive towards establishing the foundations to enable firms to develop viable FinTech solutions which drive innovation, enhance access to financial products and increase competition, whilst promoting market integrity and delivering better customer experiences and protection.

In this respect, the Malta Financial Services Authority (the “**MFSA**”) has recently announced its intention to establish Malta as an international FinTech hub which supports and enables service providers to introduce technology in their services and products, while driving and encouraging innovation at the same time.

The Government of Malta and the MFSA have, in recent years, given considerable importance to FinTech, with distributed ledger technology (“**DLT**”) taking centre stage in Malta as the next evolutionary step in business and everyday life since the internet. While most commonly associated with Bitcoin and other cryptocurrencies, DLT presents a multitude of other applications that have begun to reshape major industries, such as music, finance, transport, and healthcare. Malta has embraced this technology and enacted comprehensive legislation to assist in the regulation of this new field in a manner which provides legal certainty, while, at the same time, encouraging innovation.

Malta has been at the forefront in seeking to regulate cryptocurrencies and DLT, and was the first European Union (“**EU**”) Member State to enact a comprehensive legal framework regulating DLT, virtual financial assets (“**VFAs**”) and entities providing certain services relating to VFAs. The Maltese parliament has recently enacted three Acts – namely, the Malta Digital Innovation Authority Act (Chapter 591 of the laws of Malta), the Innovative Technology Arrangements and Services Act (Chapter 592 of the laws of Malta), and the Virtual Financial Assets Act (Chapter 590 of the laws of Malta) – which together seek to

regulate DLT, the offering and issuance of VFAs, and the provision of certain services relating to VFAs, ultimately with a view to encouraging firms to set up their businesses in a blockchain-friendly jurisdiction which does not stifle innovation.

In particular, the abovementioned Virtual Financial Assets Act regulates token offerings and the provision of certain services relating to VFAs, which are, in turn, defined by the aforementioned Act as including any form of digital medium recordation that is used as a digital medium of exchange, unit of account, or store of value and that is not (a) electronic money (which is regulated pursuant to Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions and, domestically, pursuant to the Financial Institutions Act, Chapter 376 of the laws of Malta), (b) a financial instrument (which falls within the scope of Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments or MiFID II, and which is regulated domestically pursuant to the Investment Services Act, Chapter 370 of the laws of Malta), or (c) a virtual token (being a form of digital medium recordation whose utility, value or application is restricted solely to the acquisition of goods or services, either solely within the DLT platform on or in relation to which it was issued or within a limited network of DLT platforms, and which may not be listed and traded on crypto-exchanges).

The progressive and broad-minded approach to regulating the blockchain and the cryptocurrencies world has encouraged some of the big players in the cryptocurrency and blockchain industry to set up their operations in Malta. With each development, Malta further lives up to its name of “the Blockchain Island”. Malta is also looking towards positioning itself amongst the top 10 countries in the world with a new artificial intelligence policy. In this respect, the Government of Malta has commenced a dialogue with stakeholders with a view to building awareness of the key topics and issues that would inform a national artificial intelligence framework, with the stated objectives being those of consulting on a policy that considers for ethically aligned, transparent and socially responsible artificial intelligence, identifying regulatory and fiscal measures to strengthen Malta’s appeal as a hub for foreign investment in this sector, and identifying the underlying skills base and infrastructure needed to support artificial intelligence.

The MFSA is promising to lead the FinTech industry by taking action and initiatives to drive innovation, becoming the stepping stone for innovation with the establishment of a FinTech regulatory sandbox (the “**Sandbox**”) which promotes innovation and experimentation, and supporting the development of a FinTech innovation hub (the “**Innovation Hub**”) for further stimulation of collaboration and innovation. Of particular interest is the MFSA’s plan to create a Sandbox, which is intended to provide a platform where firms may explore and test their business concepts and solutions with proportionate regulatory safeguards, in a contained environment for a well-defined duration. The Sandbox would allow the MFSA to monitor innovative upcoming businesses within a contained risk environment to safeguard customers and innovators alike.

In recognition of the fact that the regulator requires the practical insight of various parties that are involved or otherwise have experience in FinTech, the MFSA will also be working and collaborating with various stakeholders, international regulators and other interested parties to develop the FinTech sector through dialogue with those who are most interested in the development of such sector. It is also expected that the MFSA will be proactive in addressing the challenges being faced by the FinTech industry with a view to bringing about workable regulatory solutions and development. Another important aspect of this exercise

will focus on customer education, which the MFSA perceives as being key to strengthening public knowledge and confidence in FinTech.

FinTech offering in Malta

Viewed as a business-friendly location, Malta is a favoured entry point to the EU because of its robust, EU-compliant regulatory framework, diverse financial ecosystem and deep talent pool. Malta has positioned its financial services sector to serve as a European hub for many specialised services. Yet, despite its successes, Malta is taking a fresh look at its finance sector which, like its counterparts Ireland, Luxembourg and Switzerland, has felt the pressures of modern international developments and realities.

Malta's financial services industry is becoming an increasingly digital industry. Whilst recognising that the financial services sector (particularly, banking, payments, insurance and asset management) is being continuously transformed by disruptive technologies that enter the market with a promise of both better and cheaper services, Malta is also keen to attract start-ups and foreign players to base their innovation hubs on the island. The increased popularity of FinTech is being fuelled by new regulatory challenges and corresponding increased costs, pressures on financial services operators to cut costs, and increasingly technology-savvy consumers.

By positioning itself as a safe and regulated space for FinTech to grow, Malta is becoming increasingly attractive to industry players particularly in view of its relatively cheaper cost base. The opportunity of being located in one of Europe's fastest-growing financial centres, coupled with Malta's strategic geographical location and proximity to the major European markets, is becoming increasingly attractive to financial software entrepreneurs. Companies are also using Malta as a stepping stone to access nearby markets which are becoming testing grounds for new financial technologies such as VFAs and DLT, and which are increasingly recognising the benefits of DLT insofar as it creates centralised logs of information, considerably reduces (if not eliminates) the possibility of deleting or manipulating records, and lowers compliance costs.

The increased popularity and attractiveness of Malta, together with the challenges being faced by traditional financial services providers, have all driven the MFSA to embark on a mission to develop a FinTech regulatory framework with a view to regulating FinTech companies providing, in particular, payments, insurance and investment and risk management services. The MFSA has started this process by developing a regulatory framework which seeks to regulate initial VFA offerings and the provision of certain services relating to VFAs, and is now seeking to push on with adapting its financial services regulatory framework to the opportunities and challenges presented by modern technology.

In this respect, Malta will be seeking to build on its reputation as a thriving ICT hub, which has managed to attract iGaming and eCommerce operators seeking to take advantage of the fiscal, geographical and logistical benefits which Malta has to offer. Malta has seen its ICT sector blossoming into a healthy software development industry with various segments including cloud computing, mobile platforms and applications, social networking and digital gaming all contributing to its success. Most notably, the ICT sector in Malta already offers solutions and products which are used in the financial services industry, particularly banks and payment services providers.

Regulatory and insurance technology

Regulators and, particularly, service providers have always sought to combine technology and regulation with a view to addressing the regulatory challenges facing the financial

services industry. The ever-increasing and unprecedented focus on regulatory data and reporting has, however, increased the attention of all stakeholders on regulatory technology (“RegTech”) and software-based compliance solutions, and the considerable value which these add to financial services operators.

Increased regulation and resulting compliance obligations are all contributing towards increasing operational pressures on financial services operators which are, in turn, being driven towards identifying technology-based solutions which increase the overall efficiency of their operations. Financial services providers are not the only parties facing such pressures and challenges – regulators are likewise facing challenges relating to the implementation of new legislation in their domestic regulatory framework whilst also adapting existing regulation to reflect the ever-changing regulatory concerns and risks being faced by financial services operators.

The approach adopted by insurance companies in light of Solvency II may be taken as an example of the manner in which RegTech may be implemented with a view to resolving such pressures. Many European insurance providers have realised the benefits of a standardised approach which, although requiring substantial investment at implementation stage, results in an excellent return on investment notwithstanding the significant number of controls to be performed, and also reduces recurring compliance costs whilst enabling a more systematic approach towards quality control.

Major service providers and practitioners in the industry have identified the following key benefits of RegTech:

- Agility – technology may be applied and used to organise datasets.
- Speed – software drastically minimises the time required to generate reports.
- Integration – technology may also help reduce timeframes within which a solution may be set up and implemented.
- Analytics – technology may also be utilised to mine big data with a view to using that same data for multiple purposes as may be useful to a particular firm.

RegTech providers have a great opportunity to apply the abovementioned benefits for the purposes of increasing the efficiency of compliance functions and reporting in general by automating many of the relevant processes. RegTech may also maximise clarity by increasing the ability of service providers to assess, digest, analyse and interpret data, thus enabling firms to make better decisions and improve overall operations. This would necessarily require financial services firms to move away from more traditional and cumbersome approaches – typically involving spreadsheet-based systems – and adopting technology-based and automated systems.

Most firms have typically sought to supplement older technologies and systems with innovative technology, rather than replacing them in their entirety. RegTech could be an excellent opportunity for service providers to introduce new capabilities that are designed to leverage existing systems and data to produce regulatory data and reporting in a cost-effective, flexible and timely manner, whilst at the same time avoiding a drastic total departure from more antiquated systems. On the other side of the coin, RegTech should also assist regulators to maximise the use of regulatory information provided by financial services operators.

The fact that RegTech solutions tend to be cloud-based further presents several advantages, including:

- Cost-effectiveness – users are exposed to less running costs.
- Flexibility – control, access and sharing of data may be customised depending on the exigencies of the operator.

- Performance/scalability – features of the relevant system may be easily adapted, added or removed.
- Security – data encryption provides the required security to an operator.

Although firms in Malta are taking the initiative to include RegTech as part of their systems, the MFSA is currently undertaking a consultation process with stakeholders in the industry with a view to introducing and regulating the concepts of RegTech and supervisory technology (“**SupTech**”). The MFSA wishes to encourage the adoption of RegTech solutions with a view to helping firms improve their regulatory and compliance processes, and helping them comply with their obligations and licence conditions more efficiently and with greater certainty. The MFSA is itself also actively working on embracing regulatory innovation, through investment in SupTech, with a view to conducting more effective and real-time supervision of licensed entities.

The MFSA has also made it clear that it will be basing its plans relating to RegTech and SupTech on relevant European and international standards established by standard setting bodies such as the European Central Bank, the EU, the Financial Action Task Force, the Financial Stability Board, the International Organisation of Securities Commissions and the International Association of Insurance Supervisors.

More specifically, although Malta has not, as yet, taken a tactical step towards regulating the introduction of insurance technology (“**InsurTech**”), this would be next natural step for insurance companies to take, in line with the general RegTech movement being undertaken by the MFSA as outlined above. InsurTech would see the application of artificial intelligence, the Internet of Things, cloud computing and big data technology towards improving the manner in which customer data is collected and processed, ultimately with a view to insurance providers coming up with more accurate decisions regarding pricing and risk management. Such technology should also help insurance providers formulate insurance policies which can be effectively and efficiently managed and applied for the benefit of customers in a more efficient and meaningful way.

Regulatory bodies

The MFSA is the single financial services regulator in Malta which regulates and supervises credit and financial institutions, investment funds and services, trust and insurance business and, more recently, VFA issuers and VFA service providers. The MFSA is open-minded and approachable and offers face-to-face meetings with financial services providers seeking to operate in and from Malta – a level of access that is rare in other financial centres. The MFSA also seeks to collaborate and work together with service providers and practitioners alike when developing the required capabilities, capacity and frameworks to regulate new areas of financial services business.

FinTech businesses are regulated by the specific legal and regulatory framework which traditionally regulates the conduct of their respective activity. Credit institutions are regulated by the provisions of the Banking Act (Chapter 371 of the laws of Malta), financial institutions (such as lending, payment services and electronic money institutions) are regulated by the Financial Institutions Act (Chapter 376 of the laws of Malta), investment services providers and investment funds are regulated by the Investment Services Act (Chapter 370 of the laws of Malta), whilst insurance providers are regulated primarily by the Insurance Business Act (Chapter 403 of the laws of Malta). The MFSA supplements each of the aforementioned regulatory frameworks by issuing rules regulating each financial services sector. Although all of the said financial services activities have witnessed

technological developments that have created innovative FinTech business propositions, payment and electronic money-related services have seen the most technological innovation over recent years.

The MFSA is now undertaking a reform process which aims at adapting the existing financial services regulatory framework to the realities and challenges presented by FinTech. In this respect, the MFSA has commenced a consultation process with the industry and practitioners in Malta with a view to obtaining the thoughts and feedback of various industry players on the manner in which existing regulation, rules and policies should be adapted and embrace FinTech. As such, the MFSA is now focusing on introducing regulations, rules and policies which serve to address specific risks and concerns that are relevant for FinTech models, revolving principally around security and technological standards. In the meantime, the MFSA and the Government of Malta have collaborated with a view to regulating a new financial services sector involving VFA issuers and VFA service providers, as was described above.

Key regulations and regulatory approaches

The MFSA is very receptive to FinTech innovation and technology-driven financial services operators, and has chosen to adopt a very proactive approach towards new entrants by dedicating the necessary resources to meet with the promoters of FinTech businesses prior to commencing the application process, with a view to understanding their proposed model and providing valuable preliminary feedback. The approach of open dialogue and hands-on regulation has made Malta a very popular base for FinTech businesses, particularly for payment service providers and electronic money institutions.

The MFSA has also recently published a consultation document entitled “MFSA FinTech Strategy – Harnessing innovation through technology” (the “**Strategy**”), which sets out the MFSA’s vision “to establish Malta as an international FinTech hub which supports and enables financial services providers to infuse technology in product and service offerings to drive innovation”. The purpose of the Strategy is to enable key FinTech players, including but not limited to start-ups and financial services incumbents, to develop innovative solutions or provide enhanced access to financial products. The Strategy is based on the successful implementation of various initiatives across six strategic pillars; namely, regulations, ecosystem, architecture, international links, knowledge, and security.

Following in the footsteps of the Malta Gaming Authority – which had successfully implemented a sandbox for the use of DLT and the acceptance of virtual currencies within the remote gaming sector – the MFSA is now proposing a “FinTech Regulatory Sandbox”. The Sandbox would provide entities “the space to operate in a controlled but fully functional services environment in which innovative new products, services, business models and delivery mechanisms can be tested, monitored and enhanced”. Whilst rigorous regulatory requirements are laudable and encouraged to safeguard the integrity of the financial services sector and related areas, it will certainly be interesting to see the degree of flexibility in which innovators will be allowed to operate in the proposed Sandbox environment without being dissuaded by overregulation. In this regard, it is noteworthy that the MFSA has recognised regulatory proportionality as a strategic priority especially in relation to start-ups and other smaller, less complex entities.

This process will require the collaboration of various partners, including authorities, governmental ministries and agencies, academic bodies and institutions, key experts and other relevant stakeholders. Close international cooperation is envisaged to leverage best practice, drive collaboration on common challenges and make it easier for firms to operate across global borders.

Cognisant of the fact that new business models, products and services in the FinTech sphere are largely shaped by the increasing significance of data and analytics, risk management and compliance, security, digitisation, enterprise mobility, payments and enhanced customer experience, the MFSA aims to provide a tailored approach to authorisation for innovative firms. The MFSA's objective is to work with start-ups and scaling companies as well as with established global financial institutions to capture additional financial technology investment and help drive increased investment, entrepreneurship and employment across the industry. The MFSA is thus currently assessing a number of viable solutions to nurture innovation and to facilitate the industry's access to FinTech, including through the establishment of the Sandbox and supporting the development of Malta as an innovation hub.

The MFSA's consultation document presents the MFSA's vision and strategy towards developing Malta into a global FinTech hub, taking into consideration the European Commission's FinTech action plan which seeks to harness the opportunities presented by technological innovation, and the European Commission's efforts to build a true digital single market. The MFSA aims to adopt RegTech and SupTech solutions and to educate the industry as a whole on the benefits and risks of FinTech and related technologies, based on the six pillars mentioned above and as follows:

- **Regulations** – to adopt regulatory and supervisory initiatives to support innovation and improve regulatory efficiency.
- **Ecosystem** – to foster community, demand and collaboration and enhance access to finance.
- **Architecture** – to encourage collaboration through the adoption of open APIs and shared platforms.
- **International Links** – to build international links across jurisdictions to foster collaboration and trust.
- **Knowledge** – to cultivate deep talent pools and stimulate research and collaborative ideas.
- **Security** – to establish an environment that is resilient to cybersecurity threats.

Furthermore, the Sandbox is intended to provide entities with the space to operate in a controlled but fully functional financial services environment in which innovative new products, services, business models and delivery mechanisms can be tested, monitored and enhanced. It is being proposed that such entities would be closely monitored by the MFSA and would require temporary regulatory authorisation to participate. Moreover, the Sandbox would provide the MFSA with the opportunity to build its technical capacity in terms of knowledge and infrastructure while identifying the applicable financial and market risks, consumer protection measures and appropriate regulatory response.

It is envisaged that this testing environment will help in policy formation to enhance regulatory clarity and lead to the development of new regulatory frameworks where required. The MFSA is thus proposing the establishment of a regulatory and supervisory framework within which the Sandbox would operate.

The MFSA has also acknowledged the fact that start-ups and small companies make up a considerable segment of the FinTech space. As such, the MFSA intends to apply the principle of proportionality in its regulatory and supervisory capacity to facilitate entry and growth of such small entities and start-ups in this sphere.

The MFSA is seeking feedback from the industry before proceeding with detailed proposals

on the implementation of the Strategy presented in its consultation document. Such input from the industry may be provided by answering and completing a set of questions contained in an online survey, developed specifically for the purpose of facilitating major stakeholders in the industry to submit their feedback in relation to the consultation document.

Restrictions

The MFSA has identified the increasing reliance of financial services firms on technology, the increasing interconnectedness within the financial sector, and the prospect of greater concentration and herd-like behaviour, as the three main FinTech-related risks to consumers, regulated firms and financial stability in general. As such, any entity seeking to enter the FinTech sphere would be required to satisfy and comply with the MFSA's requirements and scrutiny to set up and conduct its business in and from Malta.

Although FinTech should present many benefits to consumers, there is also scope for consumers to be disadvantaged and prejudiced due to a lack of consumer understanding of the nature and risks of FinTech-related products and services, misselling of products and services, financial exclusion, lack of data privacy, security and protection and reduced competition. In this respect, the MFSA seeks to obtain a better understanding of the business model of any prospective FinTech operator with a view to ensuring that the aforementioned risks are mitigated from the relevant operations.

Furthermore, although the precise nature of risks inherent in firms depends on the types of FinTech solutions and new technologies that such firms are adopting, such risks may be broadly categorised into the following six broad categories:

- Business model viability and governance, wherein the boards and senior management of firms may not have sufficient awareness and understanding of FinTech.
- Technology risk and operational resilience.
- Data handling, wherein the inherent value of data may increase the potential for misuse, and also data limitations which may make it difficult for firms to validate outcomes, not least where artificial intelligence is used to analyse datasets and to generate solutions.
- Conduct and anti-money laundering, wherein FinTech adaptation and the resulting changes in how firms operate could result in firms struggling to meet business conduct, market dealing and anti-money laundering requirements.
- Legal, wherein some FinTech applications raise difficult legal questions, not least where cross-border operations extend across different national legal and regulatory frameworks.

The MFSA would seek to ensure that any prospective FinTech firm would adequately identify and address all of the above risks with a view to excluding or at least mitigating the same.

It is further worthy to note that the MFSA is paying increased attention to the potential risks to financial stability from a number of FinTech-related developments. There is also a more general concern of whether there is sufficient information available to accurately track the magnitude and precise nature of some of these developments. In this respect, some of the major risks which the MFSA is trying to address and restrict as much as possible relate to:

- Concentration, wherein successful FinTech firms and a small number of dominant third-party suppliers may emerge as being of systemic importance.

- Alternative channels of financial intermediation, wherein non-bank providers of credit, payment systems and other financial activities may grow rapidly while not being regulated appropriately.
- Herd-like behaviour, which may arise from the widespread use of similar machine learning and other strategies for lending or trading.
- Increased use of crypto-assets which may lead to financial instability as a result of price volatility and the potential impact of crypto-assets on payment systems.
- Vulnerabilities from the increasing levels of operational risk and cyber risk in the financial system.

Although the MFSA is still developing its regulatory strategy for FinTech business and activities, the MFSA already takes into account all of the risks which it perceives as being inherent in FinTech as was outlined above, with a view to determining whether a particular FinTech operation should be authorised, the extent of its authorisation, and the specific licence and operating conditions which should be imposed on the relevant service provider.

Cross-border business

The establishment of FinTech businesses in Malta has been on the rise. Much of Malta's success can be credited to its EU membership, which has provided firms with access to the EU's massive internal market of over five hundred million people. Malta's most important commercial relationship is with the EU. Unsurprisingly, the island is also positioning itself as a base for UK finance companies.

Certain FinTech businesses licensed in another EU or European Economic Area ("EEA") Member State may freely target and access new customers in Malta as long as they undertake the necessary prescribed regulatory notifications and processes to provide cross-border services or to establish a branch in Malta. Where, on the other hand, the FinTech business is based outside the EU or the EEA, the applicable regulatory framework would effectively prohibit any solicitation of customers based in Malta, unless the relevant business obtains authorisation from the MFSA for such purposes.

The MFSA is also seeking to build international relationships with the intention to establish FinTech bridges ("FinTech Bridges") with different jurisdictions, both within and outside of the EU and the EEA. FinTech Bridges are intended to be bilateral cooperation agreements which facilitate cross-border FinTech knowledge, adoption and investment, seek to assist in reducing barriers to market entry whilst encouraging innovation in both countries' financial services sectors by strengthening links between the regulators. Furthermore, the MFSA believes that building strong international links provides jurisdictions with the ability to collaborate on common challenges or issues which can contribute positively to the development of the global FinTech sector. These collaborations help to identify emerging FinTech trends, enabling regulators to maintain visibility over regulatory and relevant economic or commercial developments in foreign markets.

Such relationships enable closer and stronger collaboration on FinTech with foreign governments, financial regulators and the industry, locally and abroad. Through the establishment of these links, the local FinTech sector will benefit in a number of ways. It will make it easier for foreign FinTech firms to access the Maltese market and for local start-ups to scale-up through access to foreign markets, whilst also attracting opportunities for international investment to Malta.

**Dr. Karl Sammut****Tel: +356 2010 5450 / Email: ksammut@sammut.legal**

Dr. Karl Sammut is a commercial lawyer specialising in business, technology and intellectual property. He is highly sought after by companies operating in the digital economy due to his ability to integrate IP and IT knowledge with commercial and corporate expertise. Karl operates in all areas of intellectual property and technology, advising on matters relating to software, hardware, cyber security, cloud as well as data protection and privacy matters. In addition, Karl has developed strong experience in corporate law, M&A transactions and other areas of commercial law. He has also advised and assisted companies in listing their securities on the Malta Stock Exchange (IPO). Karl is a graduate in law from the University of Malta with a *Magister Juris* in EU law.

**Dr. Bradley Gatt****Tel: +356 2010 5450 / Email: bgatt@sammut.legal**

Dr. Bradley Gatt graduated with a Doctor of Laws from the University of Malta in 2005 and was admitted to the Bar in Malta in 2006. Bradley worked in the tax and legal department of one of Malta's leading audit firms as a corporate services adviser for three years, where he gained valuable experience in company law and corporate services. Before joining the firm in 2019, Bradley worked in two Maltese law firms for 10 years during which, apart from gaining additional experience in commercial and company law, his legal practice focused on financial services. Since then, Bradley has advised and assisted investment funds, fund managers and other investment services providers, banks and financial institutions, on various legal and regulatory matters relating to the setting up, authorisation and conduct of their regulated activities in Malta.

sammut.legal

Office 3, The Agora Business Centre, Triq l-Ahwa Galea, Mosta, MST 3340, Malta
Tel: +356 2010 5450 / www.sammut.legal

Mexico

Ramón Bravo Herrera, Martín Cortina Camargo & Héctor Cuevas González
Deloitte Legal (Mexico)

Approaches and developments

The regulatory developments brought about by the *'Fintech Fever'* are being assessed on their initial outcomes; countless lessons have been learned considering the opposing viewpoints of regulation and deregulation, the aftereffects of which have been both disappointing and encouraging. Looking ahead, while policymakers in Mexico do not have to set themselves the task of revolutionising financial oversight and regulatory frameworks, they must be poised to adjust the rules they have enacted with a view to achieving goals such as financial inclusion, promoting a culture of saving and investment, reducing transaction costs, preventing money laundering and terrorist financing, strengthening competition and attracting investment. In some cases, this would mean loosening regulation; and in other cases, this would imply toughening otherwise vulnerable provisions. Because of the short time frame during which the Mexican Fintech legal ecosystem has been in force and effect, surmising the costs and benefits that have arisen out of it may prove challenging; nevertheless, there is no other way to arrive at actionable insights.

In this context, the measurements carried out by the Inter-American Development Bank ('IDB') are of special interest: according to the *'Report on Fintech in Latin America 2018: Growth and Consolidation'* (IDB, 2018), notwithstanding the fact that Mexico was the first country in Latin America and the Caribbean to introduce a specific law for the Fintech sector – the *'Ley de Instituciones de Tecnología Financiera'* or *'Financial Technology Institutions Law'* (the **'Fintech Law'**), which came into force on 10 March 2018 – and while this development secured its place among the major zone's ecosystems (23% of the country's Fintech start-ups (273) are concentrated in this region), Mexico was beaten in terms of attracting investors' attention. To tell the truth, venture capital Fintech investments in the nation (USD 80 million) were as little as just over one tenth of those made in the market ranked first, Brazil (USD 859 million). Noteworthy among these is the *Konfio* SMEs credit platform financing (USD 10 million) by, *inter alia*, the International Finance Corporation.

It is important to state, however, that investment in start-ups is at a very incipient stage in the Latin America and Caribbean region, a fact which can be established if we take into account that out of all Fintech start-ups that received external funding, 79% received less than USD 500,000 (IDB, 2018). Importantly, 52% of the Fintech start-ups in Mexico concentrate on the unbanked or unserved segments, a number which, faced with the Fintech sector's prospect of increasing opportunities and enhancing financial inclusion, may be seen to have somehow fallen short of expectations. In accordance with the World Economic Forum's report *'Beyond Fintech: A Pragmatic Assessment Of Disruptive Potential In Financial Services'*, published in collaboration with *Deloitte*, this may have to do with the

fact that ‘customer willingness to switch away from incumbents has been overestimated’ (WEF, 2017) *vis-à-vis* switching costs and insufficiently material innovations.

The reason for this latter phenomenon is that, irrespective of incumbents’ requirement under the **Fintech Law** to, put broadly, provide open access to data from their customers (a feature spearheaded by Mexico), the secondary regulation concerning open banking has not yet been approved;¹ this has hindered providers’ innovation, as the development and use of application program interfaces to exchange specific data between competitors lacks adequate directions.

Indeed, this delay in the approval of secondary regulation has been the most significant challenge in the appraisal of the **Fintech Law**’s efficiency; that is, of the operational guarantees for Fintech institutions (‘**FTIs**’) it entails. Incidentally, secondary regulations, such as those published as recently as on 8, 11 and 19 March 2019, by both the ‘*Secretariat of Treasury and Public Credit*’ (*Secretaría de Hacienda y Crédito Público*; hereinafter, the ‘**SHCP**’) and the ‘*Mexican Central Bank*’ (*Banco de México*; hereinafter, the ‘**MCB**’), have inhibited cryptocurrency exchange with the general public (which will likely result in the sub-segment’s migration away from Mexico) or have introduced complicated and cumbersome requirements to set up a **FTI**, such as excessive minimum capital requirements. Moreover, some important items were altogether left out from the **Fintech Law** and its regulations, including, by way of example, robo-advisors, which are dealt with by the old-fashioned provisions of the ‘*Mexican Securities Law*’ (*Ley del Mercado de Valores*) for financial investments advisors. To produce a final panorama, even if all the preconceived secondary provisions pursuant to the **Fintech Law** have been enacted (with exception of the one regarding open banking and the use of application program interfaces), it would seem, at first glance, that these need to be slightly adjusted to remove entry barriers for **FTIs**, as well as unnecessary regulatory hurdles.

Fintech offering in Mexico

The number of Fintech start-ups grew by 52% over the last year in Mexico; interestingly, in spite of the 100% growth rate of lending, which is the chief Fintech segment in Mexico, the highest growth rate corresponded to scoring, identity, and fraud (500%): this was surely a response to the necessity of novel cyber-security technologies to counteract the risks and threats entailed by digital growth (IDB, 2018). It is important to clarify, however, that these lending start-ups to which the IDB report refers may, perhaps, be different to the crowdfunders addressed and regulated under the **Fintech Law** – i.e., different to entities that have been authorised by the ‘*National Banking and Securities Commission*’ (*Comisión Nacional Bancaria y de Valores*; hereinafter, the ‘**CNBV**’) to facilitate the channelling of funds from investors from the general public to borrowers in the form of equity, debt or co-ownership. These lending start-ups may refer to multiple purpose financial entities (*sociedades financiera de objeto múltiple* or ‘**SOFOMs**’) which may offer extended credit lines, typically microcredits, to the public without requiring authorisation from the **CNBV** to operate as a bank; which, insofar as they offer their financial products online, may qualify broadly as ‘Fintech institutions’, although not in accordance with the **Fintech Law**, as pointed out.

Evidently, traditional financial services markets are evolving into digital marketplaces. One example as to this assertion was the launch of the banking collaboration platforms and innovation programs ‘*Open Sandbox*’ and ‘*Spotlight*’ by *BBVA Bancomer* and *Santander* in 2017, which has supplied an avenue for the modernisation of traditional financial services markets in Mexico through their collaboration with **FTIs**. As outlined in the previous section, the **Fintech Law** and its regulations address some aspects of this evolution and the

disruptions thereof. The delegation of the regulation responsibility under the **Fintech Law** to financial authorities was, distinctly, a wise decision, as administrative rules can be amended much more easily than legislation in response to Fintech's developments. Another good move was the adoption of a regulatory sandbox approach in Fintech regulation (see the '*Key regulations and regulatory approaches*' section below) to enable the temporary operation of an 'innovative model' under a lenient framework.

Regulatory and insurance technology

Private initiatives have begun fostering the use of technology by supervising and regulating authorities: in 2016, the *RegTech for Regulators Accelerator* 'partnered with (...) authorities in (...) Mexico to develop tools and techniques for better market supervision and policy analysis' (Gurung and Perlman, 2018), an effort which led to the creation of an access-controlled data storage platform of the **CNBV** that automatically validates, analyses and reports data submitted by financial institutions in connection with anti-money laundering ('**AML**') requirements. Technology improvement has also moved high in the agenda of insurance companies (insuretech), particularly as regards digital sales. In 2017, AIG Mexico launched, by way of example, '*Seguro X Kilómetro*', a pay-as-you-drive insurance based 100% on telematics. The emergence of RegTech in Mexico has not been not handled specifically, from a legal perspective; however, insurance technology was recently addressed (on 26 March 2019) in secondary regulations, under an amendment (5/19) to the '*Insurance and Surety Sole Ordinance*' (*Circular Modificatoria 5/19 de la Única de Seguros y Fianzas*).

Regulatory bodies

In Mexico, a fragmented regulatory approach has applied for a while now; under this model, every type of financial entity is assigned to a different regulator. **FTIs** were put, for instance, under the supervision of the **CNBV**, which is in charge of most financial institutions, including, *inter alia*, security exchanges, and banks, the '*Insurance and Surety National Commission*' (*Comisión Nacional de Seguros y Fianzas*; hereinafter, the '**CNSF**'), which oversees the insurance and bonding sector, and the '*National Pension Savings System Commission*' (*Comisión Nacional del Sistema de Ahorro para el Retiro*; hereinafter, the '**CNSF**'), the pension funds system.

Both market conduct and prudential regulation functions have been vested in these commissions, all of which are ascribed to the **SHCP**. Consumer protection, on the other hand, including in connection with **FTIs** transactions, is handled by the '*National Commission for the Defense of Users of Financial Services*' (*Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros*; hereinafter, the '**CONDUSEF**'); this latter commission is, unlike the others, separate from the **SHCP**, a trait which could be seen as evidence supporting the existence of a twin peak model of financial system regulation in Mexico. In actual fact, prudential and market conduct functions overlap within the authority scope of the abovementioned regulators.

Additionally, from a data protection regulation perspective, **FTIs** must comply with the general framework and directives applicable to private persons, and are subject to the supervision of the '*National Institute for Transparency, Access to Information and Personal Data Protection*' (*Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*).

A further defining feature of the regulatory bodies in Mexico concerns the fact that federal legislation embraces a non-monopolist regime, in the sense that regulators are separate from

the **MCB**, which is mainly responsible for monetary policy, financial stability, and payment systems in Mexico; the **MCB** therefore also deals with macroeconomic prudential regulation of financial entities and **FTIs**, to achieve financial institutions' soundness of and overall financial system stability and protection.

The authorities in charge of the Fintech sector are, consequently, the **SHCP**, through the **CNBV**, the **MCB**, and a collegiate body: the '*Committee on Financial Technology Institutions*', which is formed by two members each from the **SHCP**, the **CNBV**, and the **MCB**.

Finally, a consultation body was also created under the '*Financial Innovation Group*' (*Grupo de Innovación Financiera*) title, to advise on the regulation and development of the Fintech sector and to coordinate the private and public sectors, as well as to establish general criteria.

Key regulations and regulatory approaches

Fintech-related legislation and regulations applicable in Mexico include:

The Fintech Law.

- '*General provisions applicable to FTIs.*'
- '*General provisions referred to under article 58 of the Fintech Law regarding the prevention and identification of transactions with illicit funds*', that is, the AML regulation issued by the **SHCP**.
- '*MCB's directive or memorandum (12/2018) to electronic payment funds institutions concerning general provisions applicable to electronic payment funds institutions transactions.*'
- '*General Provisions applicable to innovative models under the Fintech Law*' issued by the **SHCP**.
- '*General provisions regarding entities authorised to operate innovative models under the Fintech Law*' issued by the **SHCP**.
- The aforementioned amendment (5/19) to the '*Insurance and Surety Sole Ordinance*'.
- Directives 4/2019, 5/2019 and 6/2019 issued by the **MCB**, which include, respectively:
- '*General provisions applicable to credit institutions and FTIs governing virtual asset transactions.*'
- '*General provisions concerning innovative models.*'
- '*General provisions applicable to crowdfunding institutions regarding foreign currency transactions and the information reports for the MCB.*'

The influence of international organisations and initiatives is discussed briefly in the '*Cross-border business*' section below.

As suggested in the '*Fintech offering in Mexico*' section above, new Fintech developments are dealt with under a regulatory sandbox approach; pursuant to this special regime, all entities intent on operating an 'innovative model' – which, under **Fintech Law**, is any model which uses tools or technological means for performing financial services with modalities different from those existing in the market – including financial entities insofar as the provisions governing them do not allow for the corresponding model, must receive a temporary authorisation (which may not exceed two years and which may be extended for an additional year) in this respect issued by the corresponding financial authority, whether the **SHCP** or the **MCB**. For these purposes, when applicable, the governing body of either

the **CNBV**, the **CONSAR**, the **CNSF** or the **CONDUSEF** must resolve previously, when applicable, on the authorisation. Incidentally, the **Fintech Law** failed to include a ‘minimum period’ requirement concerning the authorisation, which is necessary for the entity requesting the authorisation to achieve sufficient results or to demonstrate performance that provides enough evidence to justify the inherent benefits of the ‘innovative model’ (Kurc, 2018).

Restrictions

As discussed in the introductory section, ‘Approaches and developments’, secondary provisions, specifically, ‘*General provisions applicable to credit and FTIs governing virtual asset transactions*’, have effectively inhibited cryptocurrency transactions in Mexico. It is important to stress that this prohibition extends to virtual assets (excluding national and foreign currencies) which are digital currencies, which may be used as mediums of exchange, and the ownership of which may be transferred electronically. These virtual assets, in the view of the **MCB**, are highly volatile and have an excessive price which responds most of the time to a seemingly unintelligible juncture of factors, owing to the fact they have a limited scalability and because they entail significant risks for their holders, in addition to their possible use in connection with money laundering and terrorism financing. In short, these provisions preclude credit institutions and **FTIs** from both allocating the risk of such transactions, either directly or indirectly, to customers and from performing exchange, transmission or custody services in respect of such virtual assets.

Notwithstanding the foregoing, these institutions may perform ‘internal transactions’, (i.e., activities carried out to conduct their passive, active and service transactions with customers or for their own benefit), including the activities carried out to support the international transfers of funds, insofar as the virtual assets have: (i) protocols which prevent the information units’ duplicates or their fractions becoming available for their simultaneous transmission; and (ii) clear issuance controls.

Cross-border business

Within the Latin America and Caribbean region, the ‘number of start-ups that have internationalized their operations is still low compared to their level of maturity. In particular, only 32 percent of the start-ups interviewed state they have expanded their operations beyond their national borders, compared to the 68 percent that have still not’ (IDB, 2018). In spite of this circumstance, some international organisation initiatives, such as the ‘*Ibero-American Fintech Association*’, which has gathered Spanish-speaking countries such as Colombia, Mexico, Peru, Spain, and Uruguay to promote international Fintech development, have encouraged collaboration between regulators. Furthermore, the inter-governmental *Financial Action Task Force* body, of which Mexico is a member jurisdiction, launched the ‘*FinTech and RegTech Initiative*’.

Endnote

1. Its issuance is expected in March 2020.



Ramón Bravo Herrera

Tel: +52 (55) 5080 7214 / Email: rambravo@deloittemx.com

Ramón joined Deloitte as partner in 2017; before this, Ramon was General Counsel of GE Mexico, where he participated in the creation of GE Capital, and was partner at Barrera Siqueiros y Torres Landa for more than 20 years. He has over 30 years of experience, providing legal services across corporate, finance, banking, private wealth, capital markets, M&A, aviation and public contracting law. His expertise includes international transactions, advising companies in private and public sectors. He was co-author of the 2019 'FINTECH chapter' for *'The Legal 500 Country Comparative Guide'*, the 2019 'Securitisation: Mexico' chapter for the *Chambers 'Global Practice Guide'*, and the 2019 'Trends and Developments: Mexico' for the *Chambers 'Private Wealth: Global Practice Guide'*. He is a member of the 'International Bar Association' and the 'Mexican Bar Association'.



Martín Cortina Camargo

Tel: +52 (55) 5900 1160 / Email: mcortina@deloittemx.com

Martín Cortina Camargo is a senior associate at Deloitte. He specialises in corporate law, banking law, financial services regulation, insolvency law and entertainment law. As a Mexican qualified attorney, Mr. Cortina has extensive experience in general corporate matters, including M&A, joint-ventures, real estate and private equity transactions as well as, concerning entertainment law, streaming and video-on-demand platforms, movies and series pre-production, production, co-production, licensing and distribution, live show productions, talent management and representation (in several industries), and intellectual property. He was the co-author of the 2017 'Restructuring and insolvency in Mexico: overview' of the 'Global Thomson Reuters Guide' and has written several articles covering diverse subjects. He is also author of the book 'Interest-free banking: the Islamic finance and banking alternative', which was published by Thomson Reuters (2017).



Héctor Alejandro Cuevas González

Tel: + 52 (55) 5080 7214 / Email: hcuevas@deloittemx.com

Héctor is a senior associate at Deloitte who provides consulting services and advice to domestic and multinational clients on regulatory matters; he has advised clients and participated in deals from such industries as banking, electric energy, telecommunications, mining, oil & gas, federal transportation and railways, aviation, construction and pharmaceuticals. He also has substantial experience in project finance deals; in this respect, he has advised some of the leading businesses (acting both on behalf of creditors and on behalf of sponsors). Héctor has also co-authored significant publications such as the 2013 and 2014 Mexico chapters from 'Anti-Corruption Regulation' in *Getting the Deal Through*, the 2019 'Securitisation: Mexico' chapter for the *Chambers 'Private Wealth: Global Practice Guide'*, and the 2019 'FINTECH Questions (MEXICO)' chapter, for 'The Legal 500 Country Comparative Guide'.

Deloitte Legal (Mexico)

Paseo de la Reforma 505, 28th Floor, Colonia Cuauhtémoc, Mexico City, 06500 Mexico

Tel: +52 (55) 5080 6000 / URL: www2.deloitte.com

Netherlands

Roderik Vrolijk & Soeradj Ramsanjhal
Stibbe N.V.

Approaches and developments

The Dutch regulators have embraced Fintech businesses on the Dutch markets. However, they have not developed a *sui generis* legislative framework in order to regulate these businesses. The approach they have chosen entails fitting Fintech business into existing legislative frameworks, albeit with several particularities.

The regulators utilise a number of principles in their approach towards regulating Fintech undertakings, namely:

- Regulation and supervision should be more activity-based as opposed to entity-based.
- Regulation, as well as its application, should be technology-neutral.
- Regulation should be proportional.
- Regulation and regulatory interpretations should be harmonised across EU Member States.
- Regulation should be applied with an ‘accommodating mindset’ from both legislators and regulators: when applying legislation, supervisors should interact with Fintech companies and focus on the underlying principles and purposes of legislation. The Dutch regulators strongly support the establishment of special teams (such as hubs and sandboxes) in support of Fintech and sharing experiences, best practices and outcomes between national initiatives taken by national authorities.
- Regulation, particularly if designed in a proportionate and principle-based manner, should be complemented by the development of adequate non-regulatory instruments and remedies, including civil-law/tort arrangements such as (product) liability mechanisms.
- Regulation should be developed based on a horizontal approach. The Dutch regulators strongly support horizontal actions by the European Commission, such as the current approach to Fintech.

The use of a technology-neutral approach has resulted in Fintech business falling under existing general financial regulations. However, the regulators are aware of developing Fintech markets and closely following and stimulating new initiatives.

Changes to Fintech-related regulation

The most significant proposed change is the pending implementation of the EU Fifth Anti-Money Laundering Directive ((EU) 2018/843, “**AML5**”). AML5 will bring custodian wallet providers within the scope of the harmonised anti-money laundering framework. This means that cryptocurrency exchanges will have to comply with anti-money laundering regulations.

Fintech offering in the Netherlands

The Dutch Fintech market is relatively well-developed. For an extended period of time there has been much activity with regards to technological solutions for the financial markets, with the most striking example being the payment services provider Adyen, which is currently valued at over EUR 20 billion. Furthermore, there are numerous examples of companies that provide Fintech, Regtech and Insurtech related services.

Holland Fintech is a Dutch lobby network for companies providing Fintech services. Judging by the large number of members, it is safe to say that the Dutch Fintech market is flourishing.¹

Considering that the Dutch financial services sector is heavily regulated, most of the companies that provide disruptive financial services will require a licence from either the Dutch Central Bank (*De Nederlandsche Bank*, “**DNB**”) or the Netherlands Authority for the Financial Markets (*Stichting Autoriteit Financiële Markten*, the “**AFM**”) in order to be authorised to provide regulated services. Examples are companies offering innovative investment advice or asset management solutions (‘robo-advice’), or providing innovative payment services within the scope of PSD2.

The Dutch regulator has expressed its intention to incorporate Fintech disruptions within the existing regulatory framework. However, if and where necessary, new regulations will be promulgated (e.g. the implementation of AML5 in the Netherlands).

Regulatory and insurance technology

Regtech

The Netherlands has seen a steady growth in companies providing Regtech services. The ever-growing body of requirements financial institutions must comply with (e.g. MiFID II, CRD IV, Solvency II and various AML regulations) provides Regtech companies with opportunities to automate and increase efficiency within the financial sector.

Examples of Dutch Regtech businesses include the company BearingPoint, which provides solutions specific to financial institutions across the regulatory value chain.² Another Regtech company is Open Risk. Open Risk is a provider of financial risk analysis tools and training.³ Another company, OSIS, provides a variety of tools that help the customer to comply with regulations; for example, a tool that evaluates existing portfolios on the bank’s balance sheet and helps assess new origination guidelines, the dividend policy and the distribution strategy in the context of the changing regulatory (IFRS9/CECL and Basel IV) and macro-economic environment.⁴ Another example is SecondFloor. This company provides several Solvency II services, which support insurers with compliance with the three pillars of the Solvency II Directive.⁵

Insurtech

Insurtech companies are present on the Dutch market. Outshared, for instance, is a smart insurance platform that offers insurance as a SaaS application. It offers different services ranging from system administration and analytics, customer services and campaign management to document management and claims processing.⁶ Another Insurtech company, Openclaims, offers insurers, leasing companies and fleet owners an online platform to tender and manage their customers’ motor insurance claims.⁷

We note that Dutch Insurtech companies often offer services supporting licensed insurers under outsourcing arrangements. Whilst Insurtech companies which do not carry out any

regulated insurance services themselves will not be required to obtain a licence, their outsourcing contracts with the licensed insurers typically contain provisions by which the Insurtech company is required to comply with the outsourcing requirements set out in Solvency II.

Regulatory bodies

The primary responsibility for regulating and supervising the Fintech industry lies with DNB and the AFM. The AFM and DNB deploy a twin-peaks model of supervision: the AFM is responsible for overseeing compliance with market conduct rules, whereas DNB supervises compliance with prudential rules.

Moreover, the Netherlands Authority for Consumer & Markets (*Autoriteit Consument & Markt* – “**ACM**”) is responsible for the protection of consumers and any competition issues. As regards compliance with PSD2, the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens* – “**AP**”) supervises compliance with the privacy provisions set out in PSD2.

Finally, the European Supervisory Authorities (“**ESAs**”) play a role in the regulation and supervision of financial institutions in the Netherlands. The relevant authorities are: the European Banking Authority (“**EBA**”); the European Securities and Markets Authority (“**ESMA**”); and the European Insurance and Occupational Pensions Authority (“**EIOPA**”). ESMA has direct supervisory authority in two areas, namely supervising credit rating agencies and trade repositories.

Key regulations and regulatory approaches

There is no legislation in the Netherlands that is specifically directed at Fintech businesses. The regulations relevant for those businesses can be found in various pieces of legislation. The main Dutch financial regulations are set out in the Financial Supervision Act (*Wet financieel toezicht* – “**Wft**”).

This is a very extensive legal act, which provides the framework for Dutch financial regulation and implements many of the EU Directives, such as CRD IV, MiFID II and Solvency II. Additional rules are contained in lower regulations, like the Prudential Rules Decree (*Besluit prudentiële regels* – “**Bpr**”) and the Market Conduct Supervision (Financial Institutions) Decree (*Besluit Gedragstoezicht financiële ondernemingen* – “**BGfo**”). Rules pertaining to anti-money laundering are set out in the Money Laundering and Terrorist Financing (Prevention) Act (*Wet ter voorkoming van witwassen en financiering van terrorisme* – “**Wwft**”).

When offering services to consumers, Fintech businesses may also be subject to the EU Consumer Directive, which has been implemented in the Dutch Civil Code.

Additionally, the General Data Protection Regulation must be adhered to.

Supra-national regulatory regimes or regulatory bodies

Since the Netherlands is part of the European Union, the ESAs play an important role in the regulation of the Dutch financial markets. The guidelines issued by ESMA, EBA and EIOPA are used by the AFM and DNB to interpret EU regulations and calibrate their supervisory activities. The AFM and DNB are not obliged by law to comply with the guidelines issued by the ESAs; however, in the event they choose not to comply, they need to explain why they have chosen not to do so. In practice, we see that the regulators comply with the guidelines in most cases. Additionally, the European Central Bank is an important player in

regulating Fintech, especially concerning cryptocurrencies and significant financial institutions.

Regulatory authorities' approach to new developments in Fintech

The Netherlands is an open-market economy and has always fostered innovative financial services.

The AFM and DNB want to offer room for innovation. They have set up a regulatory sandbox in order to accommodate parties that want to contribute to a more stable financial environment. They have expressly stated that financial innovation must be fostered.⁸ The AFM and DNB have also opened up an innovation hub. In this hub, experts from both organisations have joined forces to provide information to market participants about supervision and supervisory rules regarding financial services and products.

Furthermore, the Dutch regulators also use a more informal approach towards market participants. They regularly organise seminars on developments in the Fintech sector and are open to preliminary discussions.

Restrictions

There are no general restrictions on Fintech companies in the Netherlands.

However, both DNB and the AFM have taken note of developments in the crypto markets. In January 2019, they published joint advice for the Dutch parliament, recommending a Dutch national licensing regime for crypto exchange platforms and crypto wallet providers, and an amendment of the European regulatory framework to enable the offering and trading of those cryptos that are comparable to shares or bonds, which can provide opportunities for SME funding. The legislator's position on this is not yet known.

Cross-border business

Fintech companies are choosing the Netherlands to establish their headquarters and are thus having an ever-larger impact on local markets. There are many reasons for this development; a highly educated population, and a well-connected position in the global economy, to name a few. The Netherlands is home to seven of the top 100 universities in the world, according to *The Times Higher Education* Ranking. Furthermore, the Netherlands has a favourable tax regime and cooperatively-minded supervisory authorities. Brexit has evidently accelerated this process, as Amsterdam and its surrounding areas provide a viable alternative to London, in particular for payment services providers and electronic money institutions.

Fintech has been garnering more attention on a European level of late. In March 2018, the European Commission released its Fintech action plan. The plan has three goals: to harness rapid advances in technology for the benefit of the EU economy, citizens and industry; to foster a more competitive and innovative European financial sector; and to ensure the integrity of the EU financial system.⁹

The Commission wants to achieve these goals by enabling innovative business models to scale-up across the EU, through issuing clear and consistent licensing requirements, increasing competition and cooperation between market players through common standards and interoperable solutions, and facilitating the emergence of innovative business models across the EU through innovation facilitators, like regulatory sandboxes. Additionally, the European Commission wants to review the suitability of the applicable rules, ensure safeguards for new technologies in the financial sector and remove obstacles to cloud services, as well as enabling Fintech applications by means of the EU blockchain's initiative.

Finally, the plan contains a chapter on how the Commission intends to build capability and knowledge among regulators and supervisors in an EU Fintech Lab, as well as details on how the Commission wants to leverage technology to support distribution of retail investment products across the Single Market.

* * *

Endnotes

1. <https://hollandfintech.com/>.
2. <https://www.bearingpoint.com/en/>.
3. <https://www.openriskmanagement.com/>.
4. <http://www.os-is.com/>.
5. <https://www.secondfloor.com/solvency-2-reporting/>.
6. <https://insur-tech.com/Startup/outshared/>.
7. <https://www.openclaims.com/>.
8. https://www.dnb.nl/en/binaries/More-room-for-innovation-in-the-financial%20sector_tcm47-361364.pdf.
9. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0109>.

**Roderik Vrolijk****Tel: + 31 20 546 01 58 / Email: roderik.vrolijk@stibbe.com**

Advising financial institutions active both nationally and internationally, Roderik provides advice in respect of securities law and financial supervision – specialising in financial markets regulation in the broadest sense. His expertise is built on experience in Stibbe’s banking and capital markets practice in Amsterdam, where he acted on a large number of significant financing transactions, IPOs and M&A transactions in the financial services industry. Furthermore, Roderik is regularly active in the area of institutional asset management, acting for some of the world’s largest asset managers as well as for institutional investors. Roderik has a Master of Laws from Utrecht University (2008, *cum laude*). He also attended the Stibbe MBA Highlights Programme (2015). In addition, Roderik is a member of the Dutch Association for Securities Law and is a member of the editorial board of the *Dutch Financial Law Review*.

**Soeradj Ramsanjhal****Tel: +31 20 546 03 76 / Email: soeradj.ramsanjhal@stibbe.com**

Having joined Stibbe in 2014, Soeradj advises financial institutions in the Netherlands and abroad on a broad range of complex regulatory, compliance and enforcement matters. He advises on many subjects relating to market access, ongoing requirements for licensed institutions and enforcement-related issues. In addition, Soeradj has expertise with the regulatory aspects of listed companies, finance and M&A transactions, litigation, and legal aspects relevant to Fintech companies. Soeradj is part of both the Stibbe Financial Markets practice group and the Criminal Law practice group. He has a Master’s in Criminal Law from the VU University of Amsterdam and attended the Stibbe MBA Highlights Programme at INSEAD (2017). He regularly publishes articles on regulatory and enforcement-related subjects.

Stibbe N.V.

Beethovenplein 10, 1077 WM, Amsterdam, Netherlands
Tel: +31 20 546 06 06 / URL: www.stibbe.com

Nigeria

Prof. Gbolahan Elias, Ebimobowei Jikenghan & Doyinsola Love Kazeem
G. Elias & Co.

Approaches and developments in Nigeria

Financial technology (“Fintech”) has garnered significant attention from traditional financial institutions, tech start-ups and investors. The Nigerian Startup Funding Report released by TechPoint.Africa for Q1 2019 reported that Fintech companies raised 80% of the total funding of \$17.6m that Nigerian start-up companies took in Q1 2019. Regulators in Nigeria are now hard-pressed to strike a balance between creating firm regulations to keep up with the rapidly-evolving Fintech landscape on the one hand, and to actively initiate policies to support innovation on the other. Recently, the Central Bank of Nigeria (“CBN”) announced plans to set up a Collateral Management Regime to regulate the activities of Fintech firms and start-ups in Nigeria. The details of the new regime are not yet published, but it represents one of the initiatives and interventions (further discussed later in this chapter) through which Nigerian regulators attempt to foster financial inclusion, stability, integrity and consumer protection. The Fintech sector in Nigeria, although still emerging, is a fast-developing sector and the possibilities for the future are huge, as ICT now represents over 13% of the Nigerian GDP. Nigeria is transitioning into a dynamic ecosystem offering Fintech start-ups a platform to succeed and potentially grow into a multibillion-dollar industry. The Government in the past five years has shown significant interest in promoting and regulating Fintech in Nigeria.

Fintech offering in Nigeria

In January 2012, the CBN, in a bid to promote financial inclusion, introduced the cashless policy, which has led to a surge of Fintech start-ups offering solutions to make banking accessible to remote areas of Nigeria. Traditional financial service providers (banks) are also leveraging on Fintech to improve customer experience and to remain competitive in the financial services ecosystem. This has led to rapid developments in the payment services space. In fact, PWC predicted in its 2017 Fintech Survey that over 62% of customers in Nigeria would be accessing financial services via mobile applications by 2022.

The impact of disruptive technology in the Nigerian economy has been witnessed mostly in the areas of retail banking, payment services and processing, lending, investment and financial management. These areas are discussed below:

(i) Banking:

Fintech has caused a major disruption in the way and manner banks provide their services to customers, especially retail banking services. For instance, virtually all banks in Nigeria now operate mobile and online banking platforms and applications that enable customers to access banking services, such as to deposit cheques and make bill payments and withdrawals from their mobile devices and computers, without the

need to visit a banking hall. Further, the CBN, in a bid to encourage the use of technology to promote financial inclusion and enhance access to financial services in rural communities, recently introduced a new category of financial service providers, the Payment Service Banks (“PSBs”). See the Guidelines for Licensing and Regulation of Payment Service Banks in Nigeria 2018. The PSB banking model allows operators (which now, for the first time, includes subsidiaries of telecommunications companies) to provide certain banking services such as acceptance of deposits from individuals and small businesses, personal remittances of money abroad, payments, micro-savings, and withdrawal services on electronic and technology-driven platforms. Banks have also deployed Artificial Intelligence through chatbots in their mobile and online banking platforms, as well as social messaging apps such as WhatsApp and Facebook Messenger. Some players have also launched full digital banking software applications offering similar services as traditional banks. For this category of financial service providers, the existing laws and guidelines applicable to traditional banks also apply, especially regarding consumer protection, cybersecurity, anti-money laundering, and capital requirements.

(ii) Alternative lending and digital credit:

A number of tech-driven alternative lending and direct credit platforms have emerged in Nigeria. These platforms enable customers to swiftly access unsecured credit facilities at attractive rates and repayment periods online. Operators in this space use machine learning to perform real-time assessment of the credit-worthiness of a user and carry out a risk evaluation on the ability of the user to repay the loan. The algorithms usually rely on non-traditional digital data mined from the mobile phone of the user in the first instance, and credit report/history obtained from facilitators such as the credit bureau (where available) for subsequent disbursements. Notable operators in this space include Paylater, Lidy, Quickcheck and Kiakia.co.

(iii) Electronic payments:

In the past several years, payment and bill collection mechanisms in Nigeria have significantly evolved following the development of electronic payments and payment processing platforms such as Quickteller, Paga, Flutterwave, Remita and Paystack. These Payment System Providers are mainly non-banking institutions that integrate the payment side of commercial activities. Until recently, there were no regulations or guidelines governing stakeholders in this area. Interested players typically approached the CBN for an approval or “no-objection” for the given product. To address this challenge, the CBN issued the Regulation for Bill Payments in Nigeria in 2018, principally to document minimum standards for processing bill payment transactions and to ensure adequate protection for the various identified stakeholders. To further address what the CBN identified as the “operational risk dynamics within the financial system” as a result of the growing acceptability of Fintech products, the CBN issued a circular on the exposure draft of the new CBN Licensing Regime (Licence Tiering) for Payment System Providers in October 2018. The proposed regime seeks to categorise payment systems providers into three licence categories – Basic Licence, Standard Licence and Super Licence, and specifies the permissible activities and minimum capital requirements for each tier.

(iv) Public revenue collection:

The various tiers of government across Nigeria have integrated diverse Fintech players to aid in public revenue collection. For instance, in June 2017, the Federal Inland

Revenue Service introduced several electronic tax services including e-Tax Payment for the payment of all Federal Government taxes and levies through payment platforms, such as NIBSS, Remita and Interswitch. Further, all payments to the Federal Government of Nigeria and its agencies are made to its Treasury Single Account *via* the Remita online payment platform.

(v) Investment and financial management:

This is another area that has been impacted by Fintech solutions. At present, trustee and asset management companies have introduced online investment platforms that enable customers to invest in money market instruments, mutual funds and treasury bills. These include online investment platforms such as I-invest, InvestNow, and the online securities trading platform, MeritTrade. Also, the Nigerian Stock Exchange has adopted Fintech solutions in the form of automated trading system (“ATS”) for securities trading on its floor. Further, non-banking institutions have also developed online platforms that provide financial management services such as savings, expense management and invoicing to customers. Notable examples include PiggyVest and CowryWise (online savings platforms), Kliqr (an online expenses management platform) and Invoice NG (an invoicing platform).

(vi) Foreign exchange and remittance transactions:

Fintech has impacted cross-border businesses particularly with respect to foreign exchange and remittance transactions. In the foreign exchange market, the Central Bank of Nigeria recently introduced the electronic Certificates of Capital Importation (“e-CCI”) regime, pursuant to the Foreign Exchange Management (Miscellaneous Provisions) Act 1995 (“FEMMPA”) and the Foreign Exchange Manual (as Amended). E-CCIs serve as evidence of capital importation into Nigeria for investment purposes and guarantee unconditional repatriation of capital, including interest, profits and dividends for foreign investors (s. 15(4) of FEMMPA). Cross-border remittances and payments have also been impacted by Fintech practices. The CBN has also issued the Guidelines on International Mobile Money Remittance Service in Nigeria 2015, which authorise licensed operators to provide inbound and outbound international money remittance services in Nigeria through mobile phones and other hand-held devices.

(vii) Blockchain, digital currencies, crowdfunding and alternative financing:

The development of virtual or cryptocurrencies activities in Nigeria have not officially gained traction due to the unfavourable regulatory attitude. On January 12, 2017, the Securities and Exchange Commission issued a public notice on Investments in Cryptocurrencies and other Virtual or Digital Currencies by which it warned the public to desist from investing in cryptocurrencies, as these virtual currencies and their operators have not been approved by the SEC, nor have regulations been made to regulate them and protect investors. Also, the CBN on February 28, 2018 issued a press release, which reiterated its earlier January 12, 2017 Circular to Banks and Other Financial Institutions on Virtual Currency Operations in Nigeria, by which it stated that virtual currencies are not recognised as legal tender in Nigeria and are used at the peril of the user.

There has been much activity in blockchain-based solutions both from the standpoint of the regulators and Fintech players. Recently, the National Information Technology Development Agency (“NITDA”) played host to Chinese facilitators from the CBN-backed China Nigeria Blockchain Initiative aimed at stimulating the development of blockchain-based products in Nigeria. Further, in November 2018, Interswitch launched its Supply Chain Finance Module built and hosted using the Microsoft Azure

Blockchain technology to provide end-to-end visibility to entrepreneurs, financial institutions and corporate organisations for the purpose of ensuring seamless trade financing in supply chain operations.

There are currently no restrictions or registration requirements on crowdfunding platforms which enable natural persons to obtain funds from the general public in Nigeria. However, private limited liability companies (the most common mode of business organisation for Fintech companies) are restricted by law in the ways they can raise funds. Section 22(5) of the Companies and Allied Matters Act, 1990 (“CAMA”) prohibits a private company from inviting the public to subscribe to its shares. “Invitation to the Public” is defined in section 69 of the Investments and Securities Act, 2007 (“ISA”) as an offer or invitation, published by a newspaper and circulated amongst persons, to anyone who may assign the benefit of the security or to any person to acquire securities dealt in by a securities exchange. Unlike private companies, public companies can generally raise equity capital through crowdfunding platforms as they may consider appropriate. Notwithstanding the foregoing, crowdfunding platforms which allow companies to raise equity capital from the general public will qualify as Capital Trade Points. Section 315 of the ISA defines a Capital Trade Point as “*an exchange registered by the Commission pursuant to this Act, which constitutes, **maintains or provides market place facilities for bringing together purchasers and sellers of securities** or for otherwise performing, with respect to securities, the functions commonly performed by a securities exchange*”. Section 28 of the ISA prohibits capital trade points from commencing operations unless they are first registered with the SEC. To this extent, crowdfunding platforms which allow companies to raise equity capital from the general public will qualify as Capital Trade Points and will be required to comply with the regulations of the ISA and the SEC Rules relating to their operations.

Regulatory and insurance technology

There are several Regulation Technology (“RegTech”) initiatives which have been introduced by regulators in Nigeria. The Central Bank of Nigeria, in collaboration with all banks in Nigeria, on February 14, 2014 launched a unique biometric identification system for the banking industry called Bank Verification Number (“BVN”). Banks are now mandated to capture biometric details of customers and issue BVNs to their customers as part of the CBN’s Know Your Customer strategy. The BVN policy has enabled Fintech players in the digital credit space to properly identify users through their unique number throughout the financial system in Nigeria. In 2017, the CBN published the regulatory framework for BVNs and Watch-List for the Nigerian Financial System in Nigeria. The framework creates a watch-list which is a database of bank customers, identified by their BVNs, who have been involved in confirmed questionable activities. A Fintech company licensed by CBN must also comply with the CBN (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institution in Nigeria) Regulations 2013. Under these regulations, such company must adopt a policy on AML and have procedures to address any risks for customers in relation to AML and the financing of terrorism.

In addition, the underlisted financial crime laws apply to financial institutions and, by implication, Fintech businesses:

- (a) Advance Fee Fraud and other Fraud Related Offences Act 2006.
- (b) Corrupt Practices and other Related Offences Act Chapter C31, LFN 2004.

- (c) Economic and Financial Crimes Commission (Establishment, Etc.) Act).
- (d) Terrorism (Prevention) Act, 2011 (as Amended).
- (e) Money Laundering (Prohibition) Act 2011 (as Amended).
- (f) Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015.

Under the CBN’s Consumer Protection Framework, Financial Institutions (“FIs”) regulated by the CBN must safeguard the privacy of customers’ data; adopt data protection measures and implement staff training programmes to prevent the unauthorised disclosure of data.

The National Information Technology Development Agency (“NITDA”) is established pursuant to the NITDA Act, published the Nigeria Data Protection Regulation 2019 (the “NDPR”). At the time of writing, the NDPR is the latest and most significant government regulation on data protection in Nigeria. The NDPR provides that “Data Controllers”, including Fintech businesses, are required to protect the privacy of natural persons residing in Nigeria, or residing outside Nigeria but of Nigerian descent, with respect to the collection and processing of personal data. “Personal data” has been defined to mean: “information relating to an identified or identifiable natural person. It includes names, addresses, photographs, e-mail addresses, bank details, posts on social networking websites, medical information, and other identifiers such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM and others.”

Regulatory bodies

It remains difficult to succinctly map out the regulatory regime applicable to fintech companies in Nigeria due to the proliferation of regulators. The main regulatory bodies in relation to the Fintech sector are the Central Bank of Nigeria, the Nigerian Deposit Insurance Corporation, the Securities and Exchange Commission, the National Insurance Commission, the Corporate Affairs Commission, the Nigerian Communications Commission and the National Information Technology Development Agency.

- (i) The Central Bank of Nigeria:

The CBN has primary responsibility for regulating financial services in Nigeria. The CBN is the principal regulator mandated to issue licences to Banks and other financial institutions by virtue of the Banks and other Financial Institutions Act 1991 (“BOFIA”). FinTech companies offering financial services to Nigerian consumers must obtain necessary licences and comply with CBN’s applicable guidelines.

- (ii) The Nigerian Deposit Insurance Corporation (“NDIC”):

The NDIC is responsible for insuring all deposit liabilities of licensed banks and other deposit-receiving financial institutions in Nigeria. Fintech companies which are in the business of obtaining and saving money deposited by Nigerian consumers such as PSBs must be registered with the NDIC, pursuant to section 15 of the NDIC Act, 2006.

- (iii) The Securities and Exchange Commission (“SEC”):

The SEC is the securities and capital market regulator in Nigeria pursuant to the ISA, 2007. Fintech companies desirous of raising capital from the capital market must register their securities with the SEC and comply with the ISA and the rules made thereunder.

- (iv) The Corporate Affairs Commission (“CAC”):

The CAC regulates the incorporation of and official record-keeping for companies in Nigeria. See section 7 CAMA. Fintech companies (including banks) must be

incorporated at the CAC to carry on business in Nigeria except otherwise exempted from this requirement (see sections 54 and 56 of CAMA).

(v) The Nigerian Communications Commission (“NCC”):

The NCC is empowered by the Nigerian Communications Act, 2003 to regulate the telecommunication industry in Nigeria. Thus, Fintech companies offering services that involve the use of mobile networks or mobile phones are subject to NCC’s regulatory purview and must obtain requisite operating licences from the NCC. For instance, companies that operate mobile payments must be licensed by the NCC pursuant to the Licence Framework for Value Added Service (“VAS”). The NCC VAS regulation defines a VAS provider as a person or organisation engaged in the provision of value-added mobile/fixed services.

(vi) The National Information Technology Development Agency (“NITDA”):

The NITDA is responsible for creating and enforcing data protection regulations in Nigeria pursuant to the NITDA Act 2007. Recently, NITDA issued the Nigerian Data Protection Regulations 2019 which seek to safeguard the rights of natural persons to data privacy and foster the safe conduct of transactions involving the exchange of personal data.

Key regulations and regulatory approaches

Key regulations

As in the United States and South Africa, there is no single “code” legislation on the regulation of Fintech in Nigeria. However, there are several existing laws (including circulars and guidelines issued by the regulators) which apply to Fintech players as set out below:

- (i) CBN Guidelines on Mobile Money Services in Nigeria, 2015;
- (ii) CBN Guidelines for Licensing and Regulation of Payment Service Banks in Nigeria, 2018;
- (iii) CBN Regulatory Framework for the Use of Unstructured Supplementary Service Data (USSD) Financial Services in Nigeria, 2018;
- (iv) CBN Regulation for Bill Payments in Nigeria, 2018;
- (v) CBN Risk-Based Cyber-Security Framework and Guidelines for Deposit Money Banks and Payment Service Providers, 2018;
- (vi) CBN Microfinance Policy, Regulatory and Supervisory Framework, 2011;
- (vii) CBN Revised Guidelines for Finance Companies in Nigeria, 2014;
- (viii) CBN Guidelines on Operations of Electronic Payment Channels in Nigeria, 2016;
- (ix) NCC Value Added Services and Aggregator Framework, 2018;
- (x) CBN Guidelines on International Mobile Money Remittance Service in Nigeria, 2015;
- (xi) CBN Guidelines on International Money Transfer Services in Nigeria, 2014; and
- (xii) Moneylenders Laws of the respective states in Nigeria.

Other generally applicable laws and regulations include the:

- (a) Companies and Allied Matters Act, 1990;
- (b) Investment and Securities Act, 2007;

- (c) Federal Competition and Consumer Protection Act, 2018;
- (d) National Insurance Commission Act;
- (e) Money Laundering (Prohibition) Act 2011 (as Amended);
- (f) Corrupt Practices and other Related Offences Act 2000;
- (g) Economic and Financial Crimes Commission (Establishment, Etc.) Act 2004;
- (h) Terrorism (Prevention) Act, 2011 (as Amended);
- (i) Advance Fee Fraud and other Fraud Related Offences Act 2006; and
- (j) Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015.

Regulatory approaches to Fintech

The CBN, the entity tasked with the responsibility of maintaining financial stability and integrity in Nigeria, has approached the regulation of fintech by promulgating and enforcing the legislation highlighted above, as well as encouraging active stakeholder engagement. In March 2018, the CBN, along with Nigeria Interbank Settlement System, introduced a regulatory sandbox (Financial Industry Sandbox) with the aim of facilitating digital innovation by Fintech companies. The regulatory sandbox permits fintech start-ups to test their innovative ideas and solutions in a controlled environment without having to immediately satisfy the necessary regulatory requirements.

Restrictions

Given the dynamic state of innovation in the Fintech space, there is currently no comprehensively clear-cut directive from the regulators on which Fintech activities are restricted as of yet. The regulatory bodies have been responding to Fintech issues on a case by case basis. As discussed above, the CBN has adopted a cautionary stance in relation to cryptocurrencies. Similarly, in August 2016, the SEC disclosed that the lack of rules and certain inhibiting provisions in CAMA and ISA currently make equity crowdfunding a challenge in Nigeria. Consequently, the SEC expressly directed a suspension of crowdfunding activities in Nigeria pending such time when a framework is developed.

However, the Nigerian regulators, being aware of these challenges, are currently looking to other jurisdictions in search for solutions. The National Association of Securities Dealers (“NASD”), in an attempt to facilitate crowdfunding in Nigeria, expressed the intention of creating a platform where companies can pitch to venture capitalists, with the aim of possibly investing in exchange for equity in the company. The NASD has released crowdfunding guidelines and rules for proposed crowdfunding market. The CBN, however, has not issued a subsequent circular approving the guidelines issued by NASD. Further, the SEC, in a public notice issued on February 28, 2018, indicated that it is participating in the International Organization of Securities Commissions’ (“IOSCO”) efforts towards the regulation of cryptocurrencies, bitcoins and other forms of electronic currency. Also, in September 2018, the Governor of the Central Bank of Nigeria announced that the CBN and the Financial Control Authority of the United Kingdom have agreed to explore ways to develop fintech regulations in Nigeria.

Cross-border business

In recent times, Nigeria has witnessed cross-border transactional activities ranging from commercial collaboration between Fintech start-ups in different countries to Fintech players from one country setting up businesses in another country, whether in Africa or across the

globe. An example is the XendBit platform, which is a decentralised blockchain platform that enables users to trade in digital assets and securities. It is notably present in Nigeria, Ghana and South Africa. Furthermore, in 2018, one of Nigeria's leading Fintech start-ups, Paga, announced a partnership with MFS Africa in order to strengthen its entrance into the cross-border remittance market. The partnership deal is aimed at linking millions of mobile wallet users and bank account holders for seamless transactions across networks and across borders. This way, Pagawallet holders will be able to receive transfers from other mobile money users across Africa or from any money transfer operator connected to the MFS hub. In addition, Nigeria is a member of the Africa Fintech Network ("AFN"), which comprises national fintech associations from different African countries. As part of its key objectives, AFN will provide wider market access in Africa in a seamless manner for Fintechs and tech-enabled innovative products, explore innovative technology transfer and export beyond Africa to the developed world and other emerging markets, and foster multinational/cross-border fintech policy and regulatory frameworks.

Nigerian Fintech outlook 2019–2020

Fintech in Nigeria is taking on a new direction, with significant events lined up in Fintech regulation in 2019 set to pave the way for some clarity on the current regulatory framework. This year is expected to witness heightened activity in the sector, as major Mobile Network Operators (MTN, Glo, Airtel) are looking to further disrupt the banking sector by obtaining CBN licences. There has been significant traction in the micro-lending space as international investors are looking to leverage advancements in blockchain and artificial intelligence in the lending space in Nigeria.

A noteworthy development is the Fintech Association of Nigeria (FintechNGR), which is Nigeria's premier multifunctional platform for the Fintech Industry. The FintechNGR provides a collaborative space for the exchange of ideas and opportunities among entrepreneurs, venture capitalists, lawyers and government organisations. We expect to see more collaboration among key stakeholders in the Nigerian Fintech services industry through self-regulated associations.

Acknowledgment

The authors would like to thank Geoffrey Adonu and Amarachi Oji for their sterling research and contribution to this chapter.



Prof. Gbolahan Elias

Tel: +234 1 460 7890 / Email: gbolahan.elias@gelias.com

Gbolahan Elias is a Senior Advocate of Nigeria and the Presiding Partner at G. Elias & Co. He has been advising leading private equity and venture capital fund managers and investees in the financial services, telecommunications, and technology sectors on investment transactions as well as on the regulatory regime of Fintech businesses in Nigeria.

Gbolahan Elias was called to the Nigerian Bar and the New York Bar in 1981 and 1990, respectively, and has been a Senior Advocate of Nigeria (the equivalent of Queen's Counsel) since 2005. He was an associate at Cravath Swaine & Moore, a pre-eminent New York law firm, in late 1989–early 1993. Prior to that, he read law at Oxford University, England, and obtained all of his four degrees – BA (1st Class Honours), MA BCL (also 1st Class Honours), D. Phil. – from Oxford University.



Ebimobowei Jikenghan

Tel: +234 805 748 7178 / Email: ebi.jikenghan@gelias.com

Ebimobowei Jikenghan a key member of G. Elias & Co.'s technology, media and telecommunications team with experience in advising local and foreign clients on sundry regulatory issues, including on the regulatory framework for setting up payment platforms in Nigeria, the local data protection regime, regulatory aspects of various card payment software and anti-money laundering aspects of technology tools deployed for payment solutions. He is currently advising a leading African e-commerce giant on obtaining a Payment Services Provider Licence ("PSSP") from the Central Bank of Nigeria.



Doyinsola Love Kazeem

Tel: +234 807 162 0729 / Email: doyin.kazeem@gelias.com

Doyinsola is an associate at G. Elias & Co. and she currently sits on the technology, media and telecommunications team. She routinely advises local and international clients on regulatory issues concerning the formation, licensing and operational requirements for Fintech companies in Nigeria.

G. Elias & Co.

6 Broad Street, Lagos, Nigeria
Tel: +234 1 460 7890 / URL: www.gelias.com

Saudi Arabia

Suhaib Adli Hammad
Hammad & Al-Mehdar Law Firm

Approaches and developments

The recent financial technology¹ boom is not only altering the face of the existing financial market through the introduction of smart services and activities such as smart applications, cryptocurrencies, and blockchain activities, but also rapidly shifting the financial market into a digitalised smart market.

The fintech revolution has revolutionised the concept of financial services delivery to customers and businesses, affecting major banking products. As a result, banks are encouraged to take extreme imminent measures to implement fintech strategies in order to mitigate the financial loss which will undercut major retail banking businesses in the upcoming few years.

The Gulf region is encouraging the developing fintech revolution at times when the region is activating oil alternative income strategies. The adoption and implementation of a fully-fledged fintech environment across private and public sectors will not only give birth to alternative income-generating resources, but will also standardise and regularise financial transactions across the region. The result will, without doubt, enable governments to monitor financial transaction more closely.

The United Arab Emirates was originally leading the fintech revolution. However, since 2016, the Abu Dhabi Global Market (ADGM)² has started to become the Gulf Cooperation Council (GCC) fintech capital, implementing fintech regulations to become the region's incubator for fintech business. Recently this year, the ADGM launched a flexible new commercial licence for tech start-ups which enables entrepreneurs to easily operate at nominal costs.

Saudi Arabia followed and introduced sandbox programmes under its two key financial and securities governing bodies, the Saudi Arabia Monetary Agency and the Capital Market Authority. However, there has not been an introduction of new laws focused on fintech.

Fintech offering in Saudi Arabia

Hammad & Al-Mehdar is pleased to have advised and structured Halalah Company,³ a first-in-kind Saudi digital payments platform company, launched on 14 November, 2018 at AlRaida Digital City in Riyadh. Halalah, a Saudi Arabian achievement, has successfully received a licence from the Saudi Monetary Arabian Agency (SAMA) as part of the experimental permit initiative. Halalah is an alternative online payment transfer mechanism that runs through smartphone applications targeting consumers and SMEs, aiming to provide users with a simple and instant experience.

Saudi Arabia also recently approved, as part of developing fintech across the GCC, its first two fintech licences. The implementation was a result of the Capital Market Authority's

(CMA) decision, earlier this year, to approve two fintech licences for crowdfunding firm Scopeer and Riyadh-based start-up Manafa Capital. The CMA had also welcomed further fintech applications focusing mainly on the Saudi market with national shareholding and expertise in an effort to assist entrepreneurs to obtain new venture funding which will, as a result, create job opportunities in the Saudi market and place Saudi Arabia as a leader in fintech across the GCC.

Regulatory and insurance technology

There has not been any significant development in relation to InsurTech. The current available solutions are only mobile applications for insured policyholders to seek services from the insurance provider.

There has not been a disruptive solution which requires the regulators to update the current insurance regulations. Online platforms which allow users to compare and buy health insurance fall under the umbrella of insurance brokers under the applicable insurance regulations in the Kingdom.

Regulatory bodies

There are two bodies overseeing fintech specifically in the Kingdom:

- The Capital Market Authority, which is the financial regulatory authority responsible for capital markets in the Kingdom of Saudi Arabia formed by Royal Decree No. (M/30) dated 2/6/1424H (16 June, 2003). Its scope in relation to fintech solutions is limited to securities activities and it is currently focused on experimenting with crowdfunding solutions.
- The Saudi Arabian Monetary Agency, which is the Central Bank of the Kingdom of Saudi Arabia. It was established under two Royal Decrees issued on 25/7/1371H (20/4/1952). The first was No. 30/4/1/1046 provided for establishing the Saudi Arabian Monetary Authority. The second, Decree No. 30/4/1/1047, provided for the approval of the Charter of the Saudi Arabian Monetary Authority, attached to the Decree, and ordering its implementation. It is also the regulator which oversees and licenses all other financial and insurance activities, including e-wallets, payment processing gateways, insurance comparison platforms, etc.

Other regulators to consider would be the Communications and Information Technology Commission (CITC) which was formed pursuant to the Council of Ministers Decision No. (74) dated 5/3/1422H. The CITC regulates electronic transactions and sets out the mechanism to validate e-transactions and e-signatures.

Key regulations and regulatory approaches

Saudi Arabia's 2030 Vision strongly supports entrepreneurship and the enhancement of fintech services, taking a cue from its neighbour, the United Arab Emirates. As a result, on 10 January, 2018, the Board of CMA issued the "Financial Technology Experimental Permit Instructions"⁴ to enable successful applicants to test their fintech solutions and benefit from the "FinTech ExPermit".

Since both SAMA and CMA have only issued experimental type of permits and within their sandbox programmes, the current applicable regulations remain as the standard financial regulations, and they are:

- Banking Control Law, promulgated by Royal Decree No. M/5 dated 22/02/1386H

(corresponding to 11/06/1966G) (the **Banking Control Law**) and its implementing regulations and relevant circulars.

- Finance Companies Control Law promulgated by Royal Decree No. M/51 dated 13/08/1433H (the **Finance Companies Control Law**) and its implementing regulations and relevant circulars.
- E-Banking Rules, issued by the Saudi Arabian Monetary Agency in April 2010.
- Electronic Transactions Law promulgated by Royal Decree No. M/18 dated 8/3/1428H (the **Electronic Transactions Law**).

As a result, companies which plan to offer fintech solutions would apply to join the sandbox of either SAMA or the CMA depending on their scope of activities, and during the testing period they would be granted a general letter (not a licence) from SAMA or the CMA authorising them to test their solution.

Restrictions

For the purpose of obtaining a commercial registration and listing a commercial activity, the solution provider would include activities that do not require specific permits, which would include the following activities:

- Software and web development.
- E-commerce and providing e-commerce solutions (this is now a standard from the Ministry of Commerce and Investment when licensing companies that plan on generating revenue from operating an online platform).
- Developing e-payment solutions.
- Providing support services related to the above.

Fintech solutions can be tested and experimented with by the solution providers under the supervision and oversight of the relevant regulatory body. The applicant must have a solution which is ready to be launched, and must provide all the required details of its purpose to the regulatory body. Upon admittance to the sandbox programme, the regulatory body would set a period for testing, which is:

- SAMA: up to six months, which may be renewed for similar periods or terminated at SAMA's sole discretion.
- CMA: up to two years, which may be renewed for an additional period if requested by the applicant at least three months prior to the expiry of the permitted experimenting period. The applicant would request the additional period required and provide sufficient explanation as to why they need this extension.

The applicants which have been admitted to the sandbox would be granted a letter permitting them to deal with third parties, which would demonstrate to such third parties that the applicants are supported by the regulatory body in their offerings, because there are still no licences or regulations under which an applicant may operate in the market.

Cross-border business

In line with the 2030 Vision, and amid Saudi Arabia's efforts to drive development in the fintech sector as part of its plan to diversify the economy away from oil, SAMA recently launched the Fintech Saudi Initiative. The Initiative focuses on promoting Saudi Arabia as a fintech hub for investors, companies, and banks in the rise of digital transactions.

In its efforts to assist Saudi banks, the Saudi Central Bank signed a deal with U.S.-based Ripple⁵ to help banks settle payments using blockchain⁶ software. It will be interesting to monitor, in the near future, Sharia products being developed by blockchain companies and the impact this will have on financial and legal regulations in the Saudi market.

In December 2018, it was also announced that Saudi Arabia and the UAE are working on a proof of concept on a trial basis to experiment with blockchain in assisting the conducting of cross-border transfers and payments. SAMA and the Central Bank of UAE have appointed an unnamed fintech solution provider to assist in this experiment and on its implementation. It is expected that this will be completed by the end of this year.⁷

We look forward to the Fintech Saudi Initiative, which is expected, in the upcoming period, to implement an awareness of fintech, labelling Saudi Arabia as a major fintech destination hub with an emerging fintech system. The result will not only boost investment in the fintech field, but will also contribute positively towards increasing non-oil income-generating sources. It remains questionable, however, to what extent the existing Saudi regulations will be able to serve the needs of the rapidly developing fintech revolution.

* * *

Endnotes

1. A modern technology competing with traditional financial methods in the delivery of financial services. Referred to recently in the 21st century as fintech.
2. A broad-based international financial centre (IFC) for local, regional and international institutions located in Abu Dhabi, United Arab Emirates.
3. www.halalah.sa.
4. Resolution Number 1-4-2018 dated 23/4/1439H Corresponding to 10/1/2018G Based on the Capital Market Law Issued by Royal Decree No M/30 dated 2/6/1424H.
5. An American technology company which develops the Ripple payment protocol and exchange network. Originally named Opencoin and renamed Ripple Labs in 2015, the company was founded in 2012 and is based in San Francisco, California.
6. Blockchain: a digital database containing information (such as records of financial transactions) that can be simultaneously used and shared within a large decentralised, publicly accessible network. Also: the technology used to create such a database. (Source: Merriam-Webster.)
7. <https://www.bankingtech.com/2018/12/uae-and-saudi-arabia-trial-cross-border-payments-on-blockchain/>.

**Suhaib Adli Hammad****Tel: +966 92 000 4626 / Email: sh@hmco.com.sa**

Suhaib joined the law firm of Hammad & Al-Mehdar in 2009 after earning his LL.B. from the International Islamic University in Malaysia. After working for nearly a year in the interim, he then obtained an LL.M. from the University of Miami in 2010, specialising in International Business Law.

He has a vast array of international legal experience gained from working on secondment with the international firm Simmons & Simmons in London and in Dubai, as well as working for a brief period in the United States and in Malaysia during his studies.

Suhaib leads the Commercial & IP practice at Hammad & Al-Mehdar and oversees all commercial, technology, telecom, intellectual property, healthcare and life sciences-related work. Suhaib advises local and regional tech solution providers and e-commerce platforms on developing their tech, protecting it, operating it, and licensing it.

Hammad & Al-Mehdar Law Firm

King Road Tower, Level 12, Office 1209 King Abdulaziz Road, Jeddah, Saudi Arabia
Tel: +966 92 000 4626 / URL: www.hmco.com.sa

Singapore

Lim Chong Kin, Benjamin Gaw & Elizabeth Tong
Drew & Napier LLC

Approaches and developments

The Singapore government and its statutory boards, including and most notably, the Monetary Authority of Singapore (“MAS”), have identified FinTech as a potential growth area. They have launched numerous initiatives to support FinTech investment and innovation in Singapore.

Institutional developments

In 2015, the MAS formed a new FinTech & Innovation Group (“FTIG”), which is dedicated to formulating regulatory policies and developing strategies to facilitate the use of technology and innovation, so as to better manage risks, enhance efficiency, and strengthen competitiveness in the financial sector.¹

At a nation-wide institutional level, the MAS and the National Research Foundation in the Prime Minister’s Office of Singapore jointly established a FinTech Office on 3 May 2016. The FinTech Office is intended to serve as a one-stop office for all FinTech matters and to promote Singapore as a FinTech hub.² FinTech businesses may seek advice on government grants and schemes through the FinTech Office. Broadly, the grants and schemes include: (1) the Financial Sector Technology and Innovation (“FSTI”) scheme, under the purview of the MAS; (2) Capabilities Development Grant – Technology Innovation scheme, under the Info-communications Media Development Authority (“IMDA”); and (3) Startup SG Accelerator, under Enterprise Singapore (a statutory board under the Singapore Ministry of Trade and Industry).

For instance, the FSTI Proof of Concept scheme aims to promote the undertaking of experimentation within the financial services sector in Singapore, and to accelerate the development and dissemination of early-stage innovative technologies in financial services. Depending on the type of project, the MAS may provide funding support of up to 50% to 70% of the qualifying costs, up to a maximum of S\$200,000, for up to 18 months to Singapore-based financial institutions as well as technology or solution providers working with Singapore-based financial institutions for the early-stage development of innovative solutions to problems in the financial industry.³

Regulation – MAS’s principles of FinTech regulation

Apart from being the central bank of Singapore, the MAS is the key regulator overseeing the financial industry in Singapore, and has oversight over financial institutions such as banks, insurers and insurance intermediaries, capital market intermediaries, financial advisers and the stock exchange. In supporting the development of the FinTech industry in Singapore, the MAS has indicated that its role is two-fold: to provide regulation conducive to innovation

while fostering safety and security; and to facilitate the infrastructure for an innovative ecosystem and the adoption of new technologies.⁴

The MAS has also laid down some general principles underlying its approach to FinTech regulation. First, the MAS has indicated that regulation should not “front-run” innovation. Instead, it would monitor new innovative offerings, and would continually evaluate whether there is a need to step in to regulate. In addition, any regulation should be introduced when the risks arising from the new technology are material or crosses a certain threshold, and that regulation should be proportionate to the risk posed.⁵ Last, the MAS would seek to incentivise risk mitigation aspects resulting from the new technologies while restraining any new risks created.

Regulation – MAS’s FinTech regulatory initiatives

In line with its regulatory principles, the MAS has introduced a FinTech Regulatory Sandbox for financial institutions as well as new FinTech players to test innovative FinTech products or services in the production environment, but within a well-defined space and duration. Under the FinTech Regulatory Sandbox, the MAS may relax specific legal and regulatory requirements which the entity would be otherwise subject to.⁶

In addition, the MAS has issued “softer” regulatory instruments, such as guidelines, which provide interpretative guidance on the application of existing legislation to innovative FinTech solutions. These include the MAS’s Guidelines on Provision of Digital Advisory Services and A Guide to Digital Token Offerings. The MAS has also issued several guidelines outlining its expectations of FIs so as to address the risks from new technology solutions. For instance, the MAS recently issued the E-Payments User Protection Guidelines, which set out duties and responsibilities of FIs and consumers in respect of payment transactions, thereby mitigating risks from mistaken and erroneous transactions. In addition, the MAS has issued notices on technology risk management as well as risk management practices on outsourcing, e.g., to third-party cloud computing services.

In view of the new FinTech payment solutions, the MAS was also integral in introducing the new Payment Services Act 2019 (No. 2 of 2019) (“PSA”). The PSA was passed on 14 January 2019, and is tentatively expected to come into force in the second half of 2019. The PSA is a single, activity-based and risk-specific legislation for payment-related services, which consolidates existing payments regulatory frameworks and introduces new types of licensable payment services. There are now seven types of payment services regulated under the PSA, which include domestic funds transfers, e-money issuance, digital payment token services and account issuance services (which include the issuing, maintaining or operating of an e-wallet account).⁷

Infrastructure – strengthening FinTech infrastructure

From an infrastructure perspective, the MAS has introduced several major initiatives to improve the national payments infrastructure, in furtherance of its objective of creating a Smart Financial Centre. In particular, the MAS has worked with industry players such as banks to develop the Fast and Secure Transfers (“FAST”) system, which is a 24/7 real-time inter-bank funds transfer system. The MAS was also involved in implementing PayNow, which operates on FAST. PayNow enables individuals or businesses to instantly transfer money using unique identifiers such as their personal identification number or mobile phone number.⁸

To streamline multiple payment channels, the MAS introduced the Unified Point-of-Sale Terminal (“UPOS”) which can accept all major credit card brands regardless of the

technologies used (for example, whether using a smart chip, Near Field Communication technology (or “NFC”) or Quick Response (“QR”) code). Moreover, the MAS facilitated the creation of a QR code known as Singapore Quick Response Code (“SGQR”) which would be adopted by payment applications as a single unified QR code for payment. This dispenses with the need for multiple QR codes from various payment service providers to be displayed at the payment terminal.

To facilitate collaboration between traditional players and new FinTech players in the financial services industry, the MAS introduced a Financial Industry Application Programming Interface (“API”) Register, which contains 313 APIs (as of November 2018) in various functional categories such as transactions, sales and marketing. The register is updated on an ongoing basis and provides FinTech startups with a consolidated register to utilise APIs contributed by financial institutions.

The MAS has also undertaken a collaborative project termed “Project Ubin” with various local and international players, including the Bank of England and the Bank of Canada, which explores the use of distributed ledger technology for clearing and settlement of payments and securities, both within and across borders.⁹

FinTech offering in Singapore

FinTech offerings – an overview

FinTech offerings in Singapore include the operation of cryptocurrency exchanges and the offering of a digital token (also known as initial coin offerings (“ICOs”)), the development of electronic payments or funds transfer solutions, including mobile and contactless payment methods, and digital advisory services (“robo-advisers”).

Existing FinTech payments solutions

One key example of disruption is the introduction of FinTech solutions that offer mobile or contactless payments and/or fund transfers. As mentioned, a number of these FinTech solutions involve government-initiated schemes, including PayNow, SGQR and UPOS. On 10 July 2017, the PayNow service was introduced, enabling customers of any of the seven participating banks (namely, Citibank Singapore, DBS Bank/POSB, HSBC, Maybank, OCBC Bank, Standard Chartered Bank and UOB) to transfer funds directly to one another using their mobile phone number or personal identification number (i.e., NRIC/FIN), almost instantly and on a 24/7 basis, without the receiver needing to download the app. There is no need to input the recipient’s bank and account number when transferring money via PayNow. The PayNow service has been expanded (under PayNow Corporate) to include businesses which are customers of the nine participating banks (namely, Citibank Singapore, DBS Bank/POSB, HSBC, Maybank, OCBC Bank, Standard Chartered Bank, UOB, Bank of China and Industrial and Commercial Bank of China).¹⁰ PayNow Corporate allows businesses and the Singapore government to instantly pay and receive money using the organisation’s Unique Entity Number.¹¹

Contactless and cashless payment services (for example, through the use of NFC, QR codes, etc.) offered by established international players such as Apple Pay, Android Pay and Samsung Pay are also prevalent, allowing users to tap and pay for goods and services at any Visa payWave and Mastercard PayPass contactless payment terminals.¹² Other cashless mobile payment options offered by private sector players include GrabPay, Singtel Dash and Alipay. For GrabPay and Singtel Dash, deductions may be made from the users’ e-wallets when users tap their smart phones on local merchants’ contactless payment

terminals. Meanwhile, Alipay is a China-based cashless payment service provider that allows payments to be made by scanning the QR code at the payment terminal, much like PayNow.¹³

Depending on the scope of the FinTech activities, electronic payment and fund transfer solutions based on FinTech may have to comply with regulatory requirements relating to payment systems and stored value facilities under the Payment Systems (Oversight) Act (Cap. 222A). In addition, licensing requirements relating to the carrying on of a remittance business may potentially apply if the payments services provider facilitates fund transfers out of Singapore.

ICOs and cryptocurrency exchanges

Singapore is also one of the largest markets for ICOs. Notable ICOs include the ICO by blockchain startup TenX, which reportedly raised close to US\$80 million and PolicyPal, an InsurTech company which had participated in the MAS's FinTech Regulatory Sandbox in 2017.¹⁴

The MAS has stated that it may regulate digital token offerings (also known as ICOs) if the digital tokens constitute capital markets products regulated under the Securities and Futures Act (Cap. 289) ("SFA"), which include shares, debentures, units in a collective investment scheme and derivative contracts. This would depend on the characteristics and the rights attached to the digital token in the offering exercise. Where the digital tokens constitute products regulated under the SFA, the offeror may have to comply with prospectus registration requirements for the offering of the digital tokens, and licensing requirements for dealing in regulated products, under the SFA. Where the offeror is seen to be operating a platform facilitating the secondary trading of digital tokens constituting regulated products, the offeror may have to be approved or recognised by the MAS as an approved exchange or a recognised market operator, unless so exempted.

Regardless of the applicability of the SFA, the offeror would be subject to ongoing anti-money laundering and countering the financing of terrorism laws, such as the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A), Terrorism (Suppression of Financing) Act (Cap. 325). This would include a mandatory suspicious transaction reporting requirement for any person who reasonably suspects that any property or part thereof is linked to the prescribed drug dealing or serious crimes, which must be reported to the Suspicious Transactions Reporting Office of Singapore.

As mentioned, the PSA was passed on 14 January 2019 but is currently not in force. We note that the PSA provides for a licensing requirement for carrying on a business of providing certain payment services such as "account issuance services", which may be applicable to e-wallets, and "digital payment token services", which may apply to persons dealing in digital payment tokens or facilitating the exchange of digital payment tokens. Once the PSA comes into force, depending on the scope of payment services, offerors conducting ICOs or operating cryptocurrency exchanges may potentially be required to obtain a licence under the PSA to carry out such activities.

Digital advisory services (robo-advisers)

The financial advisory space in Singapore has seen several new FinTech players offering digital advisory services ("**robo-advisers**"), which are advisory services on investment products based on automated, algorithm-based tools involving limited or no human interaction. Notable robo-advisers include StashAway, Smartly, AutoWealth, MoneyOwl and Endowus.

In view of the increasing prevalence of digital advisory services, the MAS has issued the

Guidelines on Provision of Digital Advisory Services on 8 October 2018 (“**Robo-advisory Guidelines**”). In the Robo-advisory Guidelines, the MAS stated that while there is no separate authorisation regime for robo-advisers, the licensing framework under the SFA and the Financial Advisers Act (Cap. 110) (“**FAA**”) is technology-agnostic. Therefore, robo-advisers would be required to be licensed if they carry on regulated activities under the relevant legislation, unless an exemption applies. In particular, the robo-adviser would be required to obtain a financial adviser’s licence, unless otherwise exempted, if it provides financial advisory services within the ambit of the FAA. In addition, if the robo-adviser offers a platform for the execution of certain investment products, it may be required to hold a capital markets services (“**CMS**”) licence under the SFA for dealing in capital markets products. Where the robo-adviser retains some discretion over the management of the clients’ investment portfolio, a CMS licence under the SFA in fund management may be required.¹⁵

Regulatory and insurance technology

RegTech

Local banks have been utilising regulatory technology solutions to comply with their ongoing regulatory obligations, such as AML/CFT obligations. For instance, UOB has partnered with a local RegTech company, Tookitaki Holding, to enhance its anti-money laundering surveillance abilities by making sharper, smarter and swifter detection of high-risk individuals and companies and suspicious activities.

Separately, DBS has developed WealthChat in collaboration with RegTech start-up FinChat, which allows wealthy clients to interact with their relationship managers via the popular instant messaging platforms WhatsApp and WeChat, while at the same time complying with its regulatory requirements.

While the use of RegTech solutions may facilitate FinTech service providers’ compliance with their ongoing regulatory obligations, in the event of any regulatory breach, the FinTech service provider would likely be held responsible for the breach. In this regard, the FinTech service provider should undertake prudent risk management practices and when engaging a third-party RegTech service provider, should retain overall supervision and oversight. Further guidance may be obtained from the MAS’s Guidelines on Outsourcing and Technology Risk Management Guidelines.

InsurTech

Singapore is one of the largest InsurTech hubs in the Asia region.¹⁶ Singapore InsurTech companies include GoBear, an insurance plans and financial products comparison platform and Bandboo, a peer-to-peer online platform for people to co-insure one another.¹⁷

PolicyPal Network, an InsurTech start-up, is a direct insurance broker that employs machine learning and artificial intelligence to offer digital insurance policies and allow users to select and manage existing policies. Users can upload their existing policies to understand their insurance coverage and research on available policies with global insurance companies, including big names like Allianz, HSBC Insurance and AXA.¹⁸

Beside InsurTech companies, there are also notable InsurTech innovation labs in Singapore. For one, Metlife Lumenlab focuses on building new products and services grounded in technology and data to help people achieve richer and more fulfilling lives. Solaria Labs was also launched in Singapore to build and test experimental new products based on customer-centric research around emerging trends such as next-generation vehicles, connected life and the sharing economy.¹⁹

The Singapore government has recognised the potential of InsurTech. Minister Ong Ye Kung, who is also a MAS's board member, has noted the MAS's desire to continue to encourage and foster Insurance-InsurTech collaborations.²⁰ While there is currently no legislation specifically regulating InsurTech under Singapore law, InsurTech companies may be regulated under a wide range of legislation such as the FAA (i.e., Financial Advisers Act) or Insurance Act. Meanwhile, the MAS, as the regulator of the industry, has stated that it is technology-neutral and will not seek to favour one technology over another, and will monitor technological developments of the industry closely.²¹

Regulatory bodies

The specific regulatory bodies involved will depend on the nature of the entity's FinTech services or products and its business activities. The MAS is the key regulator of the financial services industry in Singapore, and administers various legislation governing financial institutions such as banks, insurers and insurance intermediaries, capital market intermediaries, financial advisers and stock exchanges. A notable exclusion from the list of financial institutions regulated by the MAS is moneylenders regulated under the Moneylenders Act (Cap. 188), which is under the purview of the Registry of Moneylenders (part of the Singapore Ministry of Law).

The Accounting and Corporate Regulatory Authority ("ACRA"), a statutory board instituted under the Singapore Ministry of Finance, is the regulator of business entities, public accountants and corporate service providers in Singapore. ACRA is responsible for the monitoring of registered companies' compliance with the Companies Act (Cap. 50), including prescribed regulatory filings and lodgments.

The Competition and Consumer Commission of Singapore ("CCCS"), a statutory board under the Ministry of Trade and Industry, administers and enforces the Competition Act (Cap. 50B), which governs competition law matters in Singapore. The CCCS also administers the Consumer Protection (Fair Trading) Act (Cap. 52A) ("CPFTA"), which is the principal consumer protection legislation in Singapore. FinTech business dealing with consumers should be aware that most MAS-regulated financial products and services come within the ambit of the CPFTA, and consumers would be able to seek redress and civil remedies for unfair practices in respect of these regulated financial products and services. In terms of matters relating to personal data protection, the Singapore Personal Data Protection Commission is the regulatory authority administering and enforcing the Personal Data Protection Act 2012 (No. 26 of 2012), which governs the collection, use and disclosure of personal data.

Different regulatory bodies may also administer FinTech-related government grants or incentive schemes. For instance, this may include the MAS (in respect of the Financial Sector Technology Innovation scheme), Enterprise Singapore (in respect of the Startup SG Accelerator, Startup SG Equity, Startup SG Founder and Startup SG Tech) and the IMDA (in respect of the Capabilities Development Grant – Technology Innovation).

Key regulations and regulatory approaches

An overview of the MAS's approach to regulatory approach and policies relating to FinTech is discussed in the section "Approaches and developments".

FinTech-related regulation

At present, there is no single omnibus legislation regulating FinTech offerings *per se*.

Existing financial services legislation is technology-agnostic and would apply to FinTech services and products if they fall within the scope of regulated financial activities. Depending on the nature of services and products, some of the following FinTech-related legislation may be applicable:

- SFA (i.e., Securities and Futures Act (Cap. 289));
- Companies Act (Cap. 50);
- Payment Systems (Oversight) Act (Cap. 222A);
- Money-changing and Remittance Businesses Act (Cap. 187);
- FAA (i.e., Financial Advisers Act (Cap. 110));
- Insurance Act (Cap. 142);
- Banking Act (Cap. 19);
- Trust Companies Act (Cap. 336);
- Moneylenders Act (Cap. 188);
- Currency Act (Cap. 69); and
- Commodity Trading Act (Cap. 48A).

Depending on the precise scope of FinTech activities, regulatory issues may include (among others):

- prospectus registration requirements for offering capital market products to persons in Singapore under the SFA;
- licensing requirements for carrying on business in regulated activities (e.g., dealing in capital markets products or fund management) under the SFA;
- regulatory requirements for operating a secondary trading facility for certain financial products under the SFA;
- regulatory requirements applicable to operators of payment systems or holders of a stored value facility under the Payment Systems (Oversight) Act;
- licensing requirements for providing financial advisory services within the meaning of the Financial Advisers Act;
- licensing requirements for operating a remittance business under the Money-changing and Remittance Business Act; and
- licensing requirements for carrying on a moneylending business under the Moneylender Act.

PSA

As stated above, the PSA has been passed but is not yet in force. The PSA will streamline the existing legislative regime for payment services by combining the Payment Systems (Oversight) Act (“PSOA”) and the Money-changing and Remittance Businesses Act (“MCRBA”) under a single legislation. In addition, the PSA expands upon the scope of regulated payment services to seven types of payment services. The PSOA and the MCRBA will be repealed at the commencement of the PSA, and Part 10 of the PSA provides for transitional arrangements to facilitate a smooth transition of existing regulated entities and entities to be regulated into the new framework.

The PSA consists of two parallel regulatory frameworks: (a) the licensing regime for payment service providers; and (b) the designation framework for significant payment systems.

With respect to the licensing regime, the PSA regulates seven types of payment services, namely:

- (a) domestic money transfer services;
- (b) cross-border money transfer services;
- (c) merchant acquisition services;
- (d) electronic money (“**e-money**”) issuance services;
- (e) digital payment token services; and
- (f) money-changing services.

Providers of such payment services will be required to hold a licence under the PSA in respect of the type of payment service that is provided, unless it is otherwise exempted from doing so.

The payment services provider would need to hold the class of licence which corresponds to the risk posed by the scale of the services provided. There are three classes of licence under the PSA, namely:

- (a) a **money-changing licence** for carrying on a business of providing money-changing services, but not any other regulated payment services;
- (b) a **standard payment institution licence** for carrying on a business of providing any regulated payment service (other than money-changing) which do not meet the thresholds set out under limb (c); and
- (c) a **major payment institution licence** for carrying on a business of providing any payment services (other than money-changing) which exceeds certain prescribed thresholds, including, for services other than e-money issuance and e-money account issuance, where the monthly average of the total value of all payment transactions that were accepted, processed, or executed exceeds: (i) S\$3 million for any one of the regulated payment services; or (ii) S\$6 million for two or more of the regulated payment services.

Where a FinTech business operates e-wallets or deals in digital payment tokens, it may be subject to the licensing requirements under the PSA once the PSA comes into effect.

Regulatory Sandbox

The MAS introduced the FinTech Regulatory Sandbox in 2016, which was intended to allow financial institutions or start-ups with a nascent FinTech service or product to experiment in a controlled environment to mitigate any financial risks. The parameters of each regulatory sandbox are tailored to address the risks posed by the FinTech service or product, and the MAS will decide on the specific regulatory requirements that may be relaxed during the sandbox period.

In 2018, the MAS proposed a Sandbox Express with fast-track approvals available within 21 days as a complement to the present FinTech Regulatory Sandbox. By doing so, the MAS seeks to encourage innovation by allowing for experiments to be embarked upon more quickly by introducing pre-defined sandboxes. This shortens the existing sandbox application and approval process because there is no longer a need for the MAS to create sandboxes specific to the applicant. In the consultation paper, the MAS has identified insurance broking, recognised market operators and remittances as the initial set of regulated activities for which pre-defined sandboxes may be designed. This list will be reviewed over time and may be amended to meet the evolving needs and interests of the financial industry as well as to address any regulatory concerns. The public consultation period for the Sandbox Express ended on 13 December 2018.

Restrictions

As stated above, the MAS's regulatory approach is to be facilitative towards innovation in the financial sector, while managing risks appropriately. Thus, the MAS has not imposed outright bans or blanket prohibitions with respect to particular FinTech activities, even where such activities have been prohibited by other jurisdictions, e.g. cryptocurrency exchanges or ICOs.

Generally, with respect to FinTech, the MAS takes a technology-neutral approach in administering and enforcing legislation. Therefore, emerging FinTech activities which come within the scope of existing activities regulated by the MAS would need to comply with such regulatory regimes. The MAS monitors Singapore's FinTech landscape and takes enforcement action to ensure such compliance.

For instance, the MAS has taken a more restrictive approach towards FinTech services which stray into shadow banking. The MAS has taken the stance that carrying on the business of taking deposits and lending to the public crosses into the territory of banking business, and upon crossing that line, a banking licence, which imposes higher regulatory standards, including capital and liquidity requirements and more stringent risk management practices, would be required. Thus, under the proposed PSA, larger e-wallet operators with an average daily e-money float of more than S\$5 million will have to ring-fence the e-money float in a prescribed manner, and will not be permitted to provide loans out of the e-money float without holding the requisite licences.²²

In line with the MAS's stated objective to help ensure that consumers are well-informed and empowered,²³ in 2017, the MAS has issued an advisory to the public on the significant risks in investments. The MAS notes that these risks include a highly speculative valuation, heightened risk of fraud and lack of a proven track record. In addition, the MAS has noted that the MAS does not regulate cryptocurrencies, and members of the public who lose money in cryptocurrency investments will not be able to rely on any protection afforded under legislation administered by the MAS.

Where FinTech activities come within the ambit of existing legislation, the MAS has shown that it is willing to take active action against errant FinTech players, so as to address any financial risks. In February 2019, the MAS warned an ICO issuer not to proceed with its securities token offering in Singapore until it can fully comply with regulatory requirements under the SFA.

The compliance with securities laws also extends to digital token exchanges. In May 2018, the MAS has issued warnings to eight digital token exchanges in Singapore not to facilitate trading in digital tokens that are deemed to be securities or futures contracts without being authorised by the MAS.

The MAS also recognised the risk that FinTech activities relating to digital tokens are prone to being misused for illegal activities due to the anonymity of the transactions, and the ease with which large sums of monies may be raised in a short period of time. Thus, the MAS and the Commercial Affairs Department (a department of the Singapore Police Force) had jointly issued a public advisory warning of the risks of digital token-related investment schemes.

Cross-border business

It was reported that FinTech investments in Singapore more than doubled, reaching US\$365 million in 2018, up from US\$180 million in 2017, placing it among the top five FinTech

markets by funds raised in the Asia-Pacific last year, according to an analysis by Accenture. Within the region, Singapore lags behind Australia, China, India and Japan.²⁴

In recognition of the potential risks and benefits arising from FinTech applications, which is virtual and may have cross-border implications, the Singapore regulators have pro-actively entered into co-operation agreements and arrangements with their foreign counterparts. For instance, in the context of cross-border payments, the MAS and the Bank of Canada have collaborated in the use of Distributed Ledger Technology (or “**DLT**”) and central bank digital currencies to make the cross-border payment process cheaper, faster and safer.

The MAS is a signatory to numerous FinTech Co-operation Agreements (approximately 30 to date) with their international counterparts which strengthen the MAS’s ability to co-operate and exchange information with foreign regulators on FinTech, as well as to promote innovation in financial services in the respective markets. For instance, in November 2018, the MAS concluded a FinTech Cooperation Agreement with the People’s Bank of China which provides for regulatory coordination with regards to the expansion of FinTech companies into each other’s markets.²⁵

To effectively monitor cross-border capital markets activities, the MAS is able to rely on a broad surveillance network which includes information from foreign securities regulators under the International Organisation of Securities Commissions Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information. Such frameworks facilitate cross-border co-operation in the area of enforcement, principally by establishing a channel for the sharing of information among the regulators.²⁶

In this regard, while FinTech services are virtual and may be borderless in nature, it should be noted that some legislation, such as the FAA and the SFA, contain provisions which give them extraterritorial effect. For instance, an act which is done entirely outside of Singapore but which has a ‘substantial and reasonably foreseeable effect’ in Singapore may still contravene the FAA or the SFA. Therefore, the offering of FinTech products and services from entities based in foreign jurisdictions to persons in Singapore may have potential regulatory implications in Singapore on the part of the offeror.

With respect to the money-laundering risks posed by FinTech activities, Singapore’s main anti-money laundering legislation, the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act expressly allows for the assertion of criminal extra-territorial jurisdiction, and empowers regulators and other government authorities such as the Suspicious Transaction Reporting Office (“**STRO**”) to exchange information and jointly co-operate in enforcement. The STRO is a member of the Egmont Group of Financial Intelligence Units (“**FIU**”), which is a forum for FIUs around the world to enhance support to their respective governments in the fight against money laundering and other serious financial crimes.²⁷

Furthermore, FinTech may result in the increase of cybercrime and cybersecurity risks, which may originate outside of Singapore, and are addressed in international co-operation arrangements. The newly-introduced Cybersecurity Act 2018 (No. 9 of 2018) and the Computer Misuse Act (Cap. 50A) sets out the framework for cross-border enforcement of cybercrime, and the Cyber Security Agency of Singapore works closely with its foreign counterparts, through information-sharing arrangements, to facilitate cybersecurity investigations.²⁸ Furthermore, the MAS has, in collaboration with the Financial Services Information Sharing and Analysis Center (“**FS-ISAC**”), established an Asia Pacific Regional Intelligence and Analysis Centre to encourage regional sharing and analysis of cybersecurity information within the financial

services sector,²⁹ and in 2017, the FS-ISAC and the MAS launched the FS-ISAC Asia Pacific Regional Analysis Centre's office and operations in Singapore.

* * *

Endnotes

1. <http://www.mas.gov.sg/news-and-publications/media-releases/2015/mas-sets-up-new-fintech-and-innovation-group.aspx>.
2. <http://www.mas.gov.sg/News-and-Publications/Media-Releases/2016/New-FinTech-Office.aspx>.
3. <http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/FSTI-Proof-Of-Concept-Scheme.aspx>.
4. <http://www.mas.gov.sg/News-and-Publications/Speeches-and-Monetary-Policy-Statements/Speeches/2016/Singapore-FinTech-Journey.aspx>.
5. <http://www.mas.gov.sg/News-and-Publications/Speeches-and-Monetary-Policy-Statements/Speeches/2016/Singapore-FinTech-Journey.aspx>.
6. <http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/FinTech-Regulatory-Sandbox/Understanding-and-applying-to-the-sandbox.aspx>. See also: <http://www.mas.gov.sg/~media/Smart%20Financial%20Centre/Sandbox/FinTech%20Regulatory%20Sandbox%20Guidelines%2019Feb2018.pdf>.
7. http://www.mas.gov.sg/~media/resource/publications/consult_papers/2017/Consultation%20on%20Proposed%20Payment%20Services%20Bill%20MAS%20P0212017.pdf.
8. <http://www.mas.gov.sg/News-and-Publications/Speeches-and-Monetary-Policy-Statements/Speeches/2018/Singapore-FinTech.aspx>.
9. <http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/Project-Ubin.aspx>.
10. <https://www.straitstimes.com/business/banking/singapore-aiming-to-become-a-cheque-free-country-by-2025-ong-ye-kung>.
11. <https://www.businesstimes.com.sg/banking-finance/paynow-corporate-seen-as-game-changer-in-singapores-cashless-drive>.
12. <https://www.straitstimes.com/tech/cashless-payment-systems-in-singapore>.
13. <https://www.straitstimes.com/tech/cashless-payment-systems-in-singapore>.
14. https://sbr.com.sg/sites/default/files/singaporebusinessreview/print/SBR_2018_Aug_Sept-26-28.pdf.
15. <http://www.mas.gov.sg/~media/MAS/Regulations%20and%20Financial%20Stability/Regulations%20Guidance%20and%20Licensing/Financial%20Advisers/Guidelines/Guidelines%20on%20Provision%20of%20Digital%20Advisory%20Services%20%20CMG%20G02.pdf>, paragraphs 12 to 14.
16. <http://fintechnews.sg/23449/insurtech/asia-100-insurtech-companies/>.
17. <http://fintechnews.sg/23449/insurtech/asia-100-insurtech-companies/>.
18. <https://www.todayonline.com/business/policypal-be-first-digitised-direct-insurance-broker>.

19. <http://fintechnews.sg/26093/fintech/top-28-fintech-and-insurtech-innovation-labs-in-singapore/>.
20. <http://www.mas.gov.sg/News-and-Publications/Speeches-and-Monetary-Policy-Statements/Speeches/2019/Opening-Address-by-Minister-Ong-Ye-Kung-at-Manulife-Tower-Opening-Ceremony.aspx>.
21. <http://www.mas.gov.sg/news-and-publications/Speeches-and-Monetary-Policy-Statements/Speeches/2018/Life-Insurance-Industry.aspx>.
22. <https://www.straitstimes.com/business/rules-to-bar-fintechs-from-moving-into-banking-ops>.
23. <http://www.mas.gov.sg/~media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/Objectives%20and%20Principles%20of%20Financial%20Supervision%20in%20Singapore.pdf> – see paragraph 17.
24. <https://www.businesstimes.com.sg/garage/singapore-fintech-investments-more-than-double-to-us365m-in-2018-amid-global-surge-accenture>.
25. <http://www.mas.gov.sg/News-and-Publications/Media-Releases/2018/Key-Agreements-Concluded-to-Enhance-Regulatory-Cooperation.aspx>.
26. <http://www.mas.gov.sg/~media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/MAS%20Capital%20Markets%20Enforcement.pdf>.
27. <http://www.mas.gov.sg/~media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/MAS%20Capital%20Markets%20Enforcement.pdf>.
28. https://www.csa.gov.sg/~media/csa/cybersecurity_bill/cybersecurity_act_faq.pdf.
29. <http://www.mas.gov.sg/News-and-Publications/Media-Releases/2016/FS-ISAC-and-MAS-Establish-APAC-Intelligence-Centre.aspx>.



Lim Chong Kin

Tel: +65 6531 4110 / Email: chongkin.lim@drewnapier.com

Chong Kin is a Director with Drew & Napier LLC. He heads the Competition and Regulatory (Contentious and Non-Contentious), and the Telecommunications, Media and Technology practices.

Chong Kin's client base spans the entire spectrum in the TMT sector, ranging from the telecoms, media, postal and other regulators, to industry players, including global telecommunication carriers, service providers, network operators, hardware manufacturers, equipment suppliers, leading global broadcasters and content providers.

Chambers 2019 lists him as a band 1 Competition and TMT lawyer, noting, "[Chong Kin] commands a leading reputation in the TMT sector and is especially noted for his regulatory expertise".



Benjamin Gaw

Tel: +65 6531 2393 / Email: benjamin.gaw@drewnapier.com

Benjamin is a Director in the Corporate & Finance Department, as well as Head of the Healthcare & Life Sciences – Corporate & Regulatory Group. He is also a member of the TMT and Employment Practices.

Benjamin's FinTech expertise includes emerging and established payments solutions, payment gateways, blockchain-based digital investment platforms, cryptocurrencies and ICOs, e-wallets, contactless and mobile payments solutions, and digital gift vouchers. Benjamin has also advised founders and investors in early-stage investments for FinTech start-ups.

Cited as a market leading lawyer by *Asialaw* for Corporate/M&A, and a recommended lawyer on *The Legal 500 Asia Pacific*. He is endorsed by Bestlawyers 2020 for Information Technology, and recognised by *Who's Who Legal 2016* as a leading lawyer for Telecommunications, Media and Technology.



Elizabeth Tong

Tel: +65 6531 2229 / Email: elizabeth.tong@drewnapier.com

Elizabeth is a Director in the Corporate & Finance Department, as well as a member of the TMT Practice Group and the Employment Practice Group.

Elizabeth regularly advises on corporate/commercial transactions and FinTech matters including on laws relating to payment systems, financial services and securities offerings in Singapore.

Elizabeth advises both MNCs and start-ups on financial regulations on first-of-its-kind payments solutions, technology platforms, e-wallets and ICOs. Elizabeth has assisted clients on matters ranging from multi-jurisdictional investments, acquisitions and restructuring projects, to complex media and technology contract negotiations.

The Legal 500 Asia Pacific recommends "fantastic" Elizabeth for her work in Telecommunications, Media & Technology Law and Employment Law, and *Asian Legal Business* identified her as one of 40 bright legal minds in the region under the age of 40.

Drew & Napier LLC

10 Collyer Quay, #10-01 Ocean Financial Centre, Singapore 049315, Singapore
Tel: +65 6535 0733 / URL: www.drewnapier.com

Slovenia

Mina Kržišnik, LL.M.
IURICORN LTD

Approaches and developments

Under the collective name Fintech, which still lacks a clear definition, financial services are understood as digital infrastructures allowing for the establishment of new solutions and new approaches to old business models; these include improvements to the traditional financial industry and innovations in the spheres of online payments, investments, fund management, money transfer, fund-raising, lending, trading, mobile banking, asset storage, capital markets, and insurance markets.

Fintech is able to deliver financial services in a new, innovative and digitalised way and facilitate peer-to-peer, multi-channel and seamless delivery of services in the financial sector, simplify access for end users via mobile applications and the internet, automate processes, strengthen the focus on customer service and enhance transparency. There are also enhanced security methods for online financial services that are necessary for consumers to feel safe switching from a physical office or broker to an online one, which include tokenisation, biometric data, and encryption. Digitisation reduces information asymmetry and levels the playing field between consumers and service providers by giving participation opportunities to the wider population. Consequently, there are more individual and institutional customers entering Fintech services, which provides more supply and demand, more liquidity and means of liquidations of a certain asset, commodity, currency, or other tradable instrument. This way, new value streams are established by creating new tradable items (for example, non-fungible tokens), new forms of value storage, new crowdfunding and financing opportunities, easier client identification worldwide, and on-the-go, new and innovative payment processing and billing solutions, and much more.

Fintech has been one of the fastest growing industries in Slovenia in recent years. On the national level, there have been many important Fintech improvements and optimisation of processes in the past, such as the introduction of mobile payments (Moneta, mBills), e-banking and mobile banking solutions, an electronic tax system (eDavki), an electronic administration system (eUprava) and electronic signatures. Furthermore, in the past three years Slovenia has seen the rise of innovative businesses and the redefinition of other traditional financial services such as saving, borrowing, investing, donating, speeding up and cheapening remittances, be it online or with a mobile device, without ever having to deal with traditional institutions, such as banks, insurance brokers and other financial institutions. The practical implications will be explained in the next section.

It is important to emphasise that traditional finances are, in most cases, redefined with implementations of new technology, namely blockchain and cryptocurrencies, artificial intelligence, machine learning and big data, and cloud computing services. These

technologies are the backbone of financial systems, not financial systems themselves. For some sectors within the financial industry, we can only change the technology behind it; for others, however (where centralisation is challenged by fast-adopting decentralisation), we may also have to change the mentality.

With regard to regulatory approaches to this new digital financial revolution, the Slovenian regulatory authorities are still quiet with regards to changing the rules. Some of them set out guidelines, opinions, recommendations, interpretations and warnings about specific Fintech-related questions, such as **initial coin offerings (ICOs)** and cryptocurrencies, electronic money and financial instruments, but this is the extent of the regulatory discussion and changes so far. No special laws or guidelines have been set out yet, which causes a certain level of legal uncertainty and unpredictability. For this reason, it is vital that each project cooperates closely with the correspondent authority.

The specific regulatory shortcomings will be debated in the following sections. As it seems, Slovenia is still rather reserved or may be waiting for other countries to make regulatory changes and then follow their example.

Fintech offering in Slovenia

Fintech's increased importance in Slovenian businesses has resulted in several successful Fintech startups and companies. It is important to know that the Fintech industry does not necessarily just mean offering new products, but also digitising old and traditional financial systems, by implementing new and disruptive technologies. Innovative solutions in Slovenia cover all areas of the financial industry, namely:

Crypto exchanges and trading platforms: One of the crypto pioneers is Bitstamp, a crypto trading platform, which redefined personal finances, investing in and enabling the buying of cryptocurrencies with fiat money (note that Bitstamp has moved its headquarters to another jurisdiction, but a part of the team remains in Slovenia). Similar trading platforms are Tokens.net (a platform for trading ERC20 tokens and other cryptocurrencies), Limitlex (a platform for bulk trading with cryptocurrencies), and Blocktrade (for trading security tokens). Slovenia is also the homeland of the core team behind the Estonian cryptocurrency exchange Kriptomat, a simple, educational and user-friendly cryptocurrency provider.

Slovenia was also one of the first countries to set up the **Bitcoin ATM** in 2014, which was developed by the company Bitnik. So far, Slovenia has altogether five of such ATMs across the country and local retail OTC offices to buy bitcoins (LoCoins).

The local **hardware vault provider** is BC vault, a Slovenian company that provides a wallet for storing cryptocurrencies, enabling users to store private keys on a secure hardware device.

The above list is rounded by the **crypto asset management companies**, such as Iconomi, which is a platform for investing in digital portfolios, and Solidum Capital, a professional crypto asset management platform.

Such platforms are disruptive, since they enable everyone to enter the world of trading and investing. In the traditional markets, investing in securities or trading commodities is harder for the wider population, as it involves a lot of bureaucracy, time, and conditions, depending on trading hours, brokers and centralised institutions and their rules, and is therefore also more costly. With the new industry, it is suddenly possible to match investors, lenders, borrowers, institutions, and regulators, which allows more people to participate in financial markets and investments worldwide and practically instantly. As already said, such marketplaces offer more liquidation means and potential liquidity, generate more value

streams in the terms of frictionless, quicker and cheaper money transfer, the creation of new digital representations of rather illiquid items (such as real estate or art pieces), popularisation of crowdfunding, and invite everyone to participate on the marketplace.

Another successful project is the **peer-to-peer finance platform** Invoice Exchange (*Borza terjatev*), digitising and simplifying invoice finance for small and medium-sized enterprises (SMEs) and setting new standards in the banking industry. The platform is disruptive since it operates as a peer-to-peer banking service, connecting corporate investors that have surplus liquidity with SMEs who are looking for working capital finance. Another **peer-to-peer invoice financing** is Hiveterminal. Their solution is a blockchain-based invoice financing platform which enables users to instantly unlock the working capital.

This disruption is also seen with **Insurtech**. The project VouchForMe (formerly InsurePal) harnesses the power of social connections among friends to reduce the costs of insurance services. The company itself is not a licensed insurance provider, but is building a global blockchain-based platform, which will disrupt the areas of motor and health insurance, property rental insurance, business transactions insurance and other areas by using the social proof concept as an alternative risk assessment method by utilising trust in the form of a financial guarantee.

The latest project, a carve-out of the Kriptomat cryptocurrency exchange, is a **token mint platform** – Kriptomat Mint Portal, a platform for minting personalised fungible or non-fungible tokens. The disruption aims to enable everyone to replace valuable items, or sensitive data, assets or rights with a less sensitive digital form. Such digital form can be used for countless cases such as access (access tokens), reward points, memberships, authentication, collectibles, licences, degrees and certification, ticketing, gifts, vouchers and coupons, among others.

It is a rather interesting fact that several of the above-named projects and companies are not set up under the Slovenian jurisdiction but elsewhere, even though such projects possess Slovenian know-how. This would probably be due to the already mentioned high level of legal uncertainty and unpredictability, and also sometimes hindering regulatory rules, which are described in the section “Restrictions” below.

In 2017 and early 2018, Slovenia has also encountered a new and popular way of fundraising through ICO events. ICOs represent a new and innovative way of attracting the general public as investors by offering them tokens in exchange for their investments. Several companies, though, did not issue tokens under the Slovenian jurisdiction, but rather opened fundraising companies in other (sometimes more favourable) jurisdictions in terms of the KYC process, taxes, costs, investment and corporate regulation.

Last but not least, Sberbank in Slovenia is teaming up with Token (a service provider that enables banks to issue and redeem payment and account data authorisations as programmable smart tokens), aiming to move beyond PSD2 compliance and towards a full embrace of open banking. Further, Bankart has released an instant payment solution via the Nordic payments processor Nets in Slovenia after obtaining final approval from the Slovenian Central Bank. Along with this technology, Bankart also aims to process regular credit transfers exchanged in files such as bill payments, salary pay-outs and pensions.

Regulatory and insurance technology

Regtech and Insurtech are both segments of Fintech. Regtech aims to address regulatory changes in financial services through innovative technology, and Insurtech is a new area of business that redefines traditional ways and procedures of policy making, policy management and insurance claims.

There have been developments in Regtech and Insurtech over the years, with the implementation of an electronic tax system (eDavki), electronic administration system (eUprava) and electronic signatures. In the fields of the prevention of money laundering, terrorist financing and tax evasion, there have been some improvements through combining cutting-edge technology and adapting to challenging legislation. For example, the online identification system ePero®START is a service for the real-time, online identification of customers with video connection on any internet-connected device.

With the advent of robots, smart contracts, powerful computers, artificial intelligence, and the Internet of Things, the insurance space needs to be transformed as well. New technology in the insurance space will change not only services, but also internal processes and the structure of employees. Decentralised insurance marketplaces, such as VouchForMe, are already seeing the light, and more and more insurance services will have to adapt to digitisation. For this reason, one of the Slovenian insurance companies – Sava Re – has entered into the prototype testing phase of blockchain, as a part of the Blockchain Insurance Industry Initiative (B3i).

Regulatory bodies

There is no uniform regulatory body in Slovenia responsible for regulating the financial field, consumer protection or prudential supervision. The regulatory system of the financial system has a mandate for micro-prudential (branch) supervision. The Bank of Slovenia, the Securities Agency (hereinafter: ATVP) and the Insurance Supervision Agency (hereinafter: AZN) can monitor each part of the Slovenian financial system. The Bank of Slovenia regulates and controls the banks, the ATVP regulates and controls the capital markets and the AZN regulates and controls the insurance companies.

However, as risks from one financial sector can rapidly affect the whole financial system, Slovenia established a special regulatory body – the Financial Stability Board. The members of the Board are representatives of the Bank of Slovenia, the Agency, the Treasury and the Ministry of Finance. The Board is responsible for the entire financial system and takes care of macro-supervision of it. Other regulators continue to carry out micro-controls of individual financial institutions. The regulations, guidelines and warnings of the above named regulatory bodies are listed in the next section.

Key regulations and regulatory approaches

The Fintech industry must follow the regular rules of the financial system, such as banking, insurance regulation, consumer protection, investment regulation, etc. Slovenia, as a part of the European Union regulatory space, must follow harmonisation efforts (by implementing Directives) and unification efforts (by following Regulations). As such, Slovenia must also follow supranational bodies and regulators, such as the European Securities and Markets Authority (ESMA), European Banking Authority (EBA) and EU Parliament guidelines, among others. The following laws are applicable to Fintech business in Slovenia:

Payment services are regulated by *Payment Services, Services for Issuing Electronic Money and Payment Systems Act* (hereinafter: ZPlaSSIED), which harmonises rules with the **Directives**: E-money Directive 2009/110/EC; Payment Services Directive (EU) 2015/2366 (PSD2); and the Directive on settlement finality in payment and securities settlement systems 98/26/ES in 2014/65/EU; and follow **Regulations**: Regulation (EC) No 924/2009 on cross-border payments; single euro payments area (SEPA) Regulation (EU) 260/2012; and Regulation 1093/2010/EU on establishing a European Supervisory Authority, among others.

Regarding financial services, Slovenia must also follow the funds transfer Regulation (EU) 2015/847 and the cash control Regulation (EC) 1889/2005.

Securities markets are regulated by the *Market in Financial Instruments Act* (ZTFI-1), which harmonises rules with the **Directives**: markets in financial instruments Directive 2014/65/EU (MiFID II); and prospectus Directive 2003/71/EC; and follow **Regulations**: markets in financial instruments Regulation (EU) 600/2014 (MiFIR); short selling Regulation (EU) 236/2012; prospectus regulation (EU) 2017/1129; and benchmark regulation (EU) 2016/1011, among others. Other European Union laws which are important to follow are the Market Abuse Directive 2014/57/EU and Market Abuse Regulation (EU) 596/2014.

Due to the complexity of the financial markets, Slovenia has several other rules in place that apply to Fintech companies, namely Ljubljana Stock Exchange Rules and Instructions and Book Entry Securities Act (ZNPV-1) – the latter implements a part of the Directive on settlement finality in payment and securities settlement systems 98/26/ES in 2014/65/EU.

Regarding post-trade services, Slovenia must follow the Derivatives Regulation (EU) No 648/2012 (EMIR), securities financing transactions Regulation 2015/2365 (SFTR), central securities depositories Regulation (EU) 909/2014 and the Financial Collateral Act (ZFZ) implementing financial collateral Directive 2002/47/EC.

Prevention of Money Laundering and Terrorist Financing is regulated by the *Prevention of Money Laundering and Terrorist Financing Act* (ZPPDFT-1) implementing the 5th AML Directive. An important piece of legislation are the Rules on determining the conditions for establishing and verifying customers' identity by means of electronic identification. The Slovenian Blockchain Think Tank community has submitted an initiative to start the process of amendments to the ZPPDFT-1 in 2018, especially with regard to the regulation of cryptocurrencies and the client identification procedure.

Investment funds are regulated by the *Investment Funds and Management Companies Act* (ZISDU-3) and *Alternative Investment Fund Managers Act* (ZUAIS), which harmonise rules with the following **Directives**: undertakings for collective investment in transferable securities Directive 2009/65/EC (UCITS); and alternative investment fund managers Directive 2011/61/EU (AIFM); and follow **Regulations**: European venture capital funds Regulation (EU) 345/2013 (EuVECA), European social entrepreneurship funds Regulation (EU) 346/2013; European long-term investment funds Regulation (EU) 2015/760 (ELTIFs); and money market funds Regulation (EU) 2017/1131, among others.

Banking services are regulated by the Banking Act (ZBan-2) and the Deposit Guarantee Scheme Act (ZSJV), which harmonise rules with the following **Directives**: banking prudential requirements Directive 2013/36/EU; bank recovery and resolution Directive 2014/59/EU; deposit guarantee schemes Directive 2014/49/EU; and financial conglomerates Directive (2002/87/EC); and follow **Regulations**: banking prudential requirements Regulation (EU) 575/2013; Credit rating agencies Regulation (EC) 1060/2009; and single supervisory mechanism Council Regulation (EU) 1024/2013, among others.

Insurance services are regulated by the *Insurance Act* (ZZavar-1), implementing **Directives**: Risk management and supervision of insurance companies Directive 2009/138/EC (Solvency 2); and insurance distribution Directive 2016/97/EU, among others.

Consumer financial services are regulated by the *Consumer Credit Act* (ZPotK-2), implementing the mortgage credit Directive 2014/17/EU, (ZPlaSSIED), payment accounts Directive 2014/92/EU, and follow the **Regulation** key information documents for packaged retail and insurance-based investment products Regulation (EU) No 1286/2014 (PRIIPs).

Personal Data Protection is regulated by the *Personal Data Protection Act (ZVOP-1)*, following the General Data Protection Regulation (EU) 2016/679, among others.

Slovenia is an innovative country with the aim of becoming the nation of startup companies as well as a blockchain hub. The authorities have written the action plan “Slovenia – the country of innovative startup companies” (hereinafter: Action Plan), where several questions regarding Fintech companies are addressed. Furthermore, regulators are actively discussing areas of Fintech, such as blockchain and cryptocurrencies, artificial intelligence and other disruptive technologies, with the help of Slovenian associations such as Bitcoin Association Slovenia, Blockchain Think Tank, and Digital Coalition Slovenia, which are actively engaged in discussions, education events and regulatory initiatives.

The approach of Slovenian regulators mainly consists of setting out guidelines, opinions and warnings, and dealing with projects on a case-by-case basis. Currently, the regulators have mainly addressed the questions of cryptocurrencies, blockchains and initial coin offerings, which are described shortly hereinafter.

The **Bank of Slovenia** has issued *Questions and answers on virtual currencies* (<https://www.bsi.si/en/media/1180/pogosta-vprasanja-in-odgovori-o-virtualnih-valutah>), in which the Bank stated that: “Virtual currencies (including cryptocurrencies such as Bitcoin) are a form of unregulated digital representation of value that is neither issued nor backed by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment, and can be transferred, stored or traded electronically.” The fact that virtual currencies do not qualify as currencies is also the European Union’s perspective; they should not be regarded as a means of payment, but as a means of exchange.

The **Financial Stability Board of the Bank of Slovenia** has issued a warning document regarding ICOs (https://bankaslovenije.blob.core.windows.net/uploaded/Finan%C4%8Dna%20stabilnost%2FOFS%2FOFS_izjava_za_javnost_glede_virtualnih_valut.docx) in which the regulators warns users of the risks to which they are exposed if they buy, store or invest in cryptocurrencies.

The **Slovenian Securities Market Agency (ATVP)** issued their position in connection with cryptocurrencies and ICOs, in the form of a consultation document of the agency regarding the matters of utility and security tokens, financial instruments, commodities and capital markets (available only in Slovenian here: http://www.a-tvp.si/Documents/Naslovnica/Povstercki/Staliska_ATVP_ICO.pdf). ATVP clearly stated that under the Slovenian law, a token is considered a transferable security only if it has been previously defined as a security, which is a record of a debt or liability that is issued as a written document or in the manner prescribed by another law. ATVP stated that current tokens on the market (such as bitcoin, Ether, Ripple, and so on) which formulate rights and obligations of token holders in an offering document (a white paper) as well in a smart contract, do not satisfy the definition of a security.

Furthermore, ATVP also tested the possibility of the ICO tokens being the collective investment undertakings under the Investment Funds and Management Companies Act. The key elements, in light of which the ATVP assesses whether the investment could be an investment fund, are:

- the absence of a general commercial or economic purpose;
- the collection of investors’ assets for the purpose of investing these assets in order to provide pooled returns to those investors;

- investing funds in accordance with predetermined investment policy; and
- owners of units as a group do not have day-to-day control over their investments.

ATVP says that the existing tokens were not issued with a view to joint investments in liquid financial investments, but primarily intended to raise funds for the implementation of certain business projects. So far, ICOs have been presented as a fundraising campaign aimed at financing the project, and the purpose of issuing tokens was not to create a combined return for investors. However, according to recent developments in the market, the possibility that some types of ICO could be considered as alternative investment funds is not excluded, under the condition that such funds are marketed and offered only to professional investors.

There was also the question of whether a token may be recognised as a money market instrument or a derivative; this definition depends on the content of a certain token. The token that does not have the content could not itself represent a money market instrument or a derivative; however, the token that functions as part of a smart contract where the content of the token is determined could potentially be treated as a money market instrument or a derivative. Depending on its content, a derivative could also be a smart deal, as portability is not required for derivative financial instruments.

The **Slovenian Financial Administration (FURS)** has issued guidelines on the tax treatment of virtual currencies and ICO events. (available only in Slovenian here: http://www.fu.gov.si/fileadmin/Internet/Davki_in_druge_dajatve/Podrocja/Dohodnina/Drugi_dohodki/Opis/Davcna_obravnava_poslovanja_z_virtualnimi_valutami_po_Zdoh-2_ZDDPO-2_ZDDV-1_in_ZDFS.docx). FURS stated that cryptocurrencies are not considered a monetary asset. Tax treatment of income derived from the operation of cryptocurrencies depends on the circumstances of the individual case.

The **Slovene Office for anti-money laundering** has issued a warning regarding bitcoin (http://www.uppd.gov.si/fileadmin/uppd.gov.si/pageuploads/dokumenti/Bitcoin_obvestilo.pdf) and guidelines on the source of funds connected to Bitcoin (http://www.uppd.gov.si/fileadmin/uppd.gov.si/pageuploads/mnenjaZPPDFT/usmeritve_virtualne_valute_izvor_sred_stev_objava_10.04.2018.docx.pdf). In connection to all kinds of cryptocurrencies, where dealing with fiat money is involved, the Office advises performing a thorough client identification, along with the source of funds check.

Restrictions

There are no specific restrictions in connection to Fintech; however, Slovenia does indeed have some legislative constraints, which may impede the development of Fintech and Fintech startups and hinder the attractiveness of Slovenia for foreign companies and investors.

Some existing laws do regulate Fintech sectors to a sufficient level, such as banking regulation, investment regulation, payment processing and electronic money regulation, and insurance laws, whereas some areas (the video identification process and regulations regarding investments in startups) are simply hindering the flourishing of Fintech or are not attractive to investors or consumers, which will be more thoroughly explained below.

Areas such as cryptocurrencies, the implications of artificial intelligence and cloud computing, the video identification process and regulations regarding investments in startups are sub-regulated and call for self-regulation, which may bring a certain differentiation in the arguments of different market players regarding an issue.

First of all, there is no regulatory arrangement of the area of cryptocurrencies, as there are quite a few successful startup companies covering the field in Slovenia. As already said,

there are stakeholders in cryptocurrency schemes such as cryptocurrency exchange platforms, storage providers (e.g. digital wallet providers) and cryptocurrency trading platforms. Fiat gateways (services that enable the buying and selling of cryptocurrencies with fiat money) and enabling withdrawals to clients' bank accounts do not need any specific licence in Slovenia, such as, for example, the Estonian digital currency licence and digital wallet licence. In Slovenia, such services are not systemically regulated and are currently supervised on a case-by-case basis. This may be good for market players up to a certain point; however, there is still a certain amount of freedom in interpretation and legal uncertainty. It also brings some amount of ambiguity regarding who is the supervisory authority to watch over Fintech companies from the perspective of the adequacy of their risk management (operational risk and cyber resilience are particularly relevant), the expertise of employees in providing the services in question, and compliance of anti-money laundering mechanisms or tax evasion mechanisms, among others. Slovenian laws do not thoroughly regulate tax questions related to issuing cryptocurrencies in an ICO event. Tax authorities use a case-by-case approach, which weakens the principle of legal safety and predictability. Additionally, the regulator has not yet set out any information about the legal treatment of STO (security token offering) events and the necessary steps for the issuer to take.

In order to attract users, many Fintech companies decide to offer services using fiat money. Such companies are entry points of fiat into the crypto world and are subject to the anti-money laundering rules, which call for client identification (Know Your Customer or KYC). Slovenian laws are rigid in prescribing an identification process which is unfavourable to businesses who aim to expand globally, and to the acquisition of international clients. Regarding products or services for which an electronic video identification of a customer can be performed, Slovenian law imposes a condition that there should be no increased risk of money laundering or terrorist financing connected to the services (such as crypto exchange) for which the obliged person is performing client identification. However, Slovenian regulatory bodies have set out warnings regarding cryptocurrencies and ICOs, which suggest all crypto-related businesses are high-risk businesses and thus are subordinated to stricter rules for the KYC process. Another restrictive measure with regard to video identification is that if a single transaction linked to a product or service exceeds EUR 15,000, the obliged person must identify and verify the identity of the client in their personal presence in accordance with the provisions of the Rules on determining the conditions for establishing and verifying customers' identity by means of electronic identification.

In case of artificial intelligence, if used in financial services such as financial or insurance advisory, Slovenia has not yet resolved the questions of liability; for example, in case a robo-advisor gives a piece of harmful advice to a consumer or refuses to give one in discriminatory circumstances. Since this sector has not yet evolved to its full potential, there is no need to regulate this area yet. When technology reaches the point where financial service providers start using autonomous tools, regulation will inevitably have to change significantly by addressing questions of formation, modification, execution, enforceability, jurisdiction, notaries and authentication, and other important questions.

Another neglected area from the legal perspective is cloud computing. There are more and more financial services provided in the cloud; however, some legal questions remain open, mostly connected to personal data security, data ownership and intellectual property. This is so especially if there are no sufficient terms and conditions or another kind of agreements put in place.

In the financial industry, it is crucial that client funds are kept separate from the company's assets. Slovenian legislation is conservative in this respect and prevents the opening of a fiduciary (segregated) bank account, in which the company can collect funds from the clients separately from their transaction or business account. This obstacle impedes the development of Fintech companies and the competitiveness of startups in this field.

In terms of investing, Slovenia has a restriction that prevents investors from investing in several companies in succession. The Companies Act (ZGD-1) sets out the limitation, namely, that one (limited liability) company may not invest in more than four companies annually. Furthermore, ZGD-1 imposes an additional obstacle for the establishing or recapitalisation of a company in Slovenia, namely that investors (angels, VCs, etc.) must be physically present in Slovenia. This last limitation greatly hinders any kind of remote cross-border investment in equity of Slovenian companies. Legislative restrictions also exist in the disinvestment and management of the shareholders of the companies. Startup companies do not normally generate profits in the first few years, and in cases where one of the founders or investors wishes to withdraw from a startup company, this is not possible under the Slovenian law if the company is operating with a loss. Last but not least, there are no tax reliefs for investors, neither legal nor natural persons, in startup companies such as in other EU countries, and the amounts of investments are upwards limited. Such protective measures might sometimes be good for investors, but in the long term it inhibits the attraction of new cash flows and encourages the use of other ways of investing (for example, ICOs, initial exchange offerings, etc.).

Another obstacle could potentially be the taxation of shares of a non-listed company. If a startup sells a part of or a whole company, they receive shares of a non-listed foreign company (acquirer) instead of paying in cash or liquid shares listed on the stock exchange. The problem is that such a startup is obliged to pay income tax, even if the shares are not liquid and before such shares can be converted to cash or become liquid on the stock exchange.

Cross-border business

Fintech is indeed disrupting Slovenian business and is transforming traditional financial services, as well as supporting services, such as legal services, education, etc. The Faculty of Commercial and Business Sciences has started to teach a new course, "The use of blockchain technology and cryptocurrencies", which is one of the first such cases in Slovenia.

There are several communities and associations cooperating closely with international stakeholders, such as the Luxembourg-Slovenian FinTech initiative, Digital Coalition, Blockchain Think Tank, Bitcoin Association Slovenia, Blockchain Alliance Europe, Noordung Blockchain Hub, etc. Slovenia is closely collaborating with regulators from other Member States and Fintech market players, and often hosts important international events, such as conferences, roundtables, summits, etc.

In March 2018, Slovenia unveiled a bitcoin monument on a roundabout in the city of Kranj. The bitcoin symbol was chosen by the bitcoin community of the city. This gesture shows not only the increased interest and importance of cryptocurrencies and blockchain technology, but also the readiness of this small country to participate in and lead the new era of digital transformation.

**Mina Kržišnik, LL.M.****Tel: +386 4023 8562 / Email: mina.krzisnik@iuricorn.com**

Mina Kržišnik is the founder of the law firm IURICORN. Her practice is focused on digital law and covers Fintech, blockchain and cryptocurrencies, artificial intelligence, cloud computing, data privacy and adjacent areas. Her clients include startups as well as corporations implementing new technologies into the business process.

She completed a Master's degree at the Erasmus University Rotterdam (the Netherlands) in commercial and corporate law, and passed the state Bar exam in 2014. Her extensive experience as a lawyer in law firms as well as in multinational corporations as an in-house lawyer helped her accumulate a wide knowledge in corporate law, international trade and transactions.

She is one of the top fintech legal advisors and strategists in the area. She is the chief legal officer and legal advisor in several ICO and STO projects, crypto exchanges, fund management portfolios and other high-tech companies.

IURICORN LTD

Zgornje Pirniče 94, 1215 Medvode, Slovenia
Tel: +386 4023 8562/ URL: www.iuricorn.com

Spain

Guillermo Yuste de Ayala
Andersen Tax & Legal Iberia, S.L.P.

Approaches and developments

There have been two major developments affecting the regulation of Fintech over the last few months.

The first development is the long-awaited transposition of the second payment services directive by means of the Payment Services Act, RDL 19/2018 of 23 November (the “**Payment Services Act**”). This enactment is primarily important since it recognises two new payment services (payment initiation services and account information services) and the possibility to access both the payment accounts in order to render payment initiation services, and the account information in order to render the account information services, respectively. While neither of these features are unique to Spain, as they are expressly provided in the Payment Services Directive (EU) 2015/2366 (“**PSD2**”), their importance in our jurisdiction may be regarded as comparatively greater than in other jurisdictions with a more evolved Fintech sector than Spain.

At the time of the transposition – and this situation continues today – payment services providers in Spain did not have access to payment settlement systems, nor any legal provision that could force the incumbent operators to grant access to their systems to third parties. As a consequence of this, the provision of payment services by operators that were not linked to incumbent operators was almost restricted to the performance of wire transfers.

Likewise, the constraints resulting from the inability to gain access to client information was a significant hurdle for those entities which were aiming to provide big data or management of personal finance.

The second development was the Council of Ministers’ approval on 22 February 2019 of the draft bill of measures for the digital transformation of the financial system, which provides for a regulatory sandbox (the “**Sandbox Bill**”). The works on this draft bill were halted as a result of the general elections held last April. However, the outcome of the general elections (where the governing party was successful) and the broad consensus in respect of the project throughout all the political spectrum allow us to have grounded expectations as to the project being approved by the courts without very significant changes. A detailed explanation of the regulatory sandbox currently envisaged by the draft bill is provided in the “Key regulations and regulatory approaches” section below.

It is also worth mentioning that the Government, prior to the elections, undertook certain steps to promote the start-up environment, thus benefitting Fintechs. These regulatory efforts, however, are way less developed than the regulatory sandbox project.

Fintech offering in Spain

There are some 400 Fintechs in Spain, covering a wide variety of verticals, and in different stages of development. Some of the most important verticals existing to date (per number of companies) are:

1. Lending.
2. Payment services, for both domestic and international payments. Micropayments are also very popular in Spain.
3. Investment companies
4. Tax and accounting solutions.
5. Personal finance.

Certain verticals, such as crypto-assets and distribution of financial products, are more common in other EU countries than in Spain.

Regulatory and insurance technology

As regards the some 100 entities providing or developing technological solutions in the Regtech sector in Spain, some of the main activities comprise:

1. Digital onboarding, for natural persons and small and medium enterprises, by using optical character recognition (“OCR”), authentication factors and digital signatures.
2. Document management, which includes automated classification of documents and extracting relevant information.
3. Provision of digital evidence.
4. Compliance services.
5. Cyber-security.
6. Credit scoring both based in financial and non-financial data (sources of behavioural data such as social networks).

As regards Insurtech, the following activities may be worth highlighting:

1. Damage prevention systems. This includes technology which is aimed at tracking the behaviour of the policyholder, and will provide incentives for correct behaviour. A good example of this is Vidamovida, launched by El Corte Inglés group, which tracks the walking habits of the policyholder, thus offering a reduction in the premia for those policyholders with healthier habits.
2. Services related to the distribution of insurance, such as hiring insurance policies or comparing offers.
3. Customer services, such as claim management and evidencing and assessing the existence of damages.
4. Fraud detection techniques.

Regulatory bodies

In Spain, the financial sector does not have a single regulatory body. There are three regulators, for financial institutions, capital markets and insurance companies, respectively.

- (i) The Bank of Spain (*Banco de España*) (“**BoSP**”) is the entity responsible for matters related to credit institutions, as well as banking activities, payment services, and electronic money.

- (ii) The National Stock Market Commission (*Comisión Nacional del Mercado de Valores*) (“**CNMV**”) is the entity responsible for matters related to stock markets and investment activities in such markets.
- (iii) The General Directorate for Insurance (*Dirección General de Seguros*) (“**GDI**”) is the entity responsible for matters related to insurance.

The CNMV is the most active regulator as regards Fintech. It addresses the queries that companies may have in connection with regulatory matters, and keeps an updated document containing its criteria in respect of the questions commonly asked. According to its portal, as of 31 December 2018, 258 queries had been raised to the CNMV, the vast majority of which dealt with crowdfunding (75) and crypto-assets and blockchain (63).

It should be noted that the notion of “regulator” is somehow misleading in our jurisdiction, since the CNMV, the BoSp and the GDI have limited regulatory powers. The legal framework affecting the finance and insurance sector arises from Parliament, from the Government directly or from the Economy Office. The “regulators” are in fact more supervisors than regulators, and have very broad inspection powers.

Aside from the sector-specific regulators, there are two other public bodies which are very relevant for the performance of financial activities:

- (i) The Spanish Data Protection Agency. While each EU Member State has its own equivalent, it is worth highlighting that historically, the Spanish Data Protection Agency has been very proactive when enforcing the applicable laws and imposing the corresponding penalties. As from the new EU regulation on data protection, which came in force on 25 May 2018, three penalties have already been imposed.
- (ii) The Spanish Commission for the Prevention of Money Laundering and Terrorism Financing. Its executive service (generally referred to as “**SEPBLAC**”) is the Spanish supervisor and intelligence unit as regards money laundering.

Key regulations and regulatory approaches

Aside from the general rules that may apply to any company, there are certain laws of specific importance to the Fintech sector. We will first make reference to such laws and, secondly, we will refer to those that are most important for each of the most significant verticals in the Spanish market. Finally, we will provide a summary of the provisions foreseen in the Sandbox Bill.

Laws of specific importance

- (i) **Data protection:** as regards data protection, the most significant rules are Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 which applies throughout the EU, and the Organic Act 3/2018 of 5 December on data protection and guaranteeing digital rights.
- (ii) **Money laundering prevention:** Act 10/2010 of 28 April, for the prevention of money laundering and terrorism financing, as amended, and its implementing regulation, RD 304/2014, of 5 May.
- (iii) **IP:** the Intellectual Property Act enacted by Royal Legislative Decree 1/1996 of 12 April, as amended. This is specifically relevant for software. Conversely to other jurisdictions, software is generally not patentable. The protection system is similar and contained in the same act that governs the protection of literary works.
- (iv) **Consumer protection:** For obvious reasons, the Act on Distance Trade of Financial Services with Consumers 22/2007 is specifically relevant for verticals.

(v) **Internet services providers:** Information Society Services Act 34/2002, of 11 July.

Most significant regulations by verticals

Provision of technological services to investment services entities or other regulated entities

This activity is not regulated and the CNMV has expressly confirmed that no authorisation is required, but if the services rendered by the technology provider imply the outsourcing of important or essential operative functions of the investment services company, the technological services provider shall be bound to cooperate with the authorities to facilitate their supervision.

It is also worth mentioning that the outsourcing of operative functions may not reach a point where it can be established that the technological services provider is indeed rendering the regulated activity: this will result in a penalty being imposed by the relevant supervisor.

Banking, personal finance, payments and transactions

(i) *Banking.* Banking, understood as the activity of obtaining reimbursable funds from the public, is a very heavily regulated activity in the EU, and most of the applicable laws and regulations either arise directly from the EU and apply directly EU-wide via EU regulations, or have been harmonised by means of EU directives. The domestic law governing the performance of banking activities is the Organisation, Supervision and Solvency of Credit Institutions Act 10/2014 of 26 June, and its developing regulation RD 84/2015 of 13 February. The existing legal framework imposes heavy requirements for the authorisation and operation of credit institutions, including a minimum share capital fully paid up of €18 million. As a consequence, most banking activity related to the Fintech sector in Spain is sponsored by incumbent players.

(ii) *Online lending.* Lending, on a general basis, is not a regulated activity. As a consequence of the lack of legal barriers, consumer finance is a very popular activity in the Fintech environment. Of course, consumer protection regulations such as the 1908 Usury Act or the Consumer Credit Act 16/2001 of 24 June are applicable. Mortgage loans are subject to the recent Real Estate Credit Act 5/2019 of 15 March, and are particularly unsuitable for direct lending due their new and particularly harsh regulations, alongside the specific formalities required for the creation of mortgages in Spain.

(iii) *Personal finance.* This vertical basically comprises two different activities: (a) assistance in the management of personal finance; and (b) comparing financial products.

The activity under (a) above is not *per se* a regulated one, but pursuant to the provisions of the recently enacted Payment Services Act, the service of offering account information (i.e. facilitating aggregated information on one or more payment accounts owned by the user) is now a regulated activity, and thus service is essential for the provision of assistance in the management of personal finance. In addition to this, if the advice included recommendations of financial products, it would not be considered financial advice (defined in section 140.1 (g) of the Stock Market Act (“SMA”) as amended and restated by RDL 4/2015 of 23 October), and would require a specific authorisation.

The activity under (b) above is also not regulated, but could be considered a regulated activity if it entails brokerage activities.

(iv) *Payment services.* Payment services are a regulated activity harmonised EU-wide by means of the PSD2, transposed by the Payment Services Act. It may be performed either by payment services institutions or by banks. As of today, no access to the banking settlement systems is available for these entities in Spain.

- (v) *Issue of electronic money.* The activity of issuing electronic money is also a regulated activity that may be performed by credit institutions or by certain specific institutions aimed at such purpose, is governed by the Electronic Money Act 21/2011 of 26 July, and requires a share capital of €350,000. As of today, no access to the banking settlement systems is available for these entities in Spain.
- (vi) *Currency exchange services.* Currency exchange services may be provided either by credit institutions or by foreign exchange establishments (*establecimientos de cambio de moneda*), regulated under Regulation RD 2660/1998. To date, these establishments require a minimum share capital of €60,000. Offering derivatives such as forward exchange may fall within the scope of regulated activities to be rendered by an Investment Services Entity and, thus, require the incorporation of a Securities Agency, although it could be exempt should the forward exchange merely act as hedging to cover the exchange risk of the currency exchanged by the client.

Investment and securities services

- (i) *Robo advice.* This activity is considered an investment service which shall be governed both by the SMA and its developing regulations. This activity is reserved to investment services companies, and the type of entity that meets the minimum legal requirements for this activity is the Financial Advice Enterprise (*Empresa de Asesoramiento Financiero*), regulated under Circular 10/2008.
- (ii) *Negotiation platforms.* When platforms are intended for the receiving and transmitting of purchase orders, or executing such orders in the market, they will be performing a regulated activity that may only be performed by securities companies (which may operate in their own name and on their behalf, or in the name of and on the behalf of third parties) or securities agencies (which may only operate in the name of and on behalf of third parties). Both entities, in addition to the relevant provisions of the SMA, are regulated by RD 217/2008.
- (iii) *Automatised portfolio management.* The management of securities portfolios is also a regulated investment service that needs to be provided by an investment services company. Among the available possibilities in Spain, the one subject to fewer regulatory requirements is the portfolio management entity (*Entidad Gestora de Carteras*), regulated by RD 217/2018, which requires a minimum share capital of €50,000.
- (iv) *Social trading.* The CNMV has made public its criterion that social trading, understood as operating an online platform where the investment strategies followed by other investors or managers may be replicated by their clients in their own portfolios, is an investment service. More precisely, the service of discretionary portfolio management is regulated under Section 140.1 d) of the SMA and 5 d) of Regulation RD 217/2008 and, consequently, can be rendered by an investment services company in the form of a portfolio management entity. However, pursuant to the document “ESMA/2012/382 MIFID Questions and Answers”, if (a) there is a specific authorisation of the client for each and every transaction order, or (b) the client determines the criteria whereby the system will convey the transaction orders, such activity shall not be considered discretionary portfolio management. The sector is clearly against the consideration of social trading as a regulated activity, and social trading platforms generally seek to benefit from the existing exemptions.

Crowdfunding

The activity of crowdfunding, defined as putting in contact through web pages or other

means those persons who offer financing in exchange for a return with counterparties who demand such financing, is a regulated activity in Spain, governed by the Promotion of Entrepreneurial Finance Act 5/2015. This activity may only be performed by crowdfunding platforms that need to be authorised by the CNMV. The forms of crowdfunding that are provided for under Spanish law are:

- (i) Crowdlending, performed by means of loans.
- (ii) Equity crowdfunding, performed by means of the issue of shares in private limited companies (which according to Spanish law are not securities), or shares or convertible bonds, so long as these do not fall within the obligation to file a prospectus by the issuer.

Collateralised crowdfunding is not prohibited under Spanish law. However, the crowdfunding platform may not receive such collateral in its own name, either on its own behalf or in the name of and on behalf of its investors. This poses severe difficulties for the creation of security and its enforcement under Spanish law.

The current regulation of crowdfunding platforms has been severely criticised, since it is considered too limitative in certain aspects, among others:

- (i) Collecting the required payments from investors to sponsors and *vice versa* is not automatically allowed, but will require a specific authorisation for the provision of payment services.
- (ii) Although the existing regulations allow the possibility of performing equity crowdfunding, the possibility to run a market where the securities subject to investment may be transferred is also excluded.
- (iii) The scope of activities and means that may be financed by means of crowdfunding platforms: general corporate finance is excluded, and other forms of financing, such as commercial paper discount, are not possible.

Crypto-assets

As of today, neither crypto-assets nor the activities related to them have specific regulation in Spain. This, however, does not mean that the issuing or trading of crypto-assets may be performed freely. A more detailed explanation of the situation as regards crypto-assets is described under the heading “Crypto-assets” below.

The Sandbox Bill

Requirements to access the Sandbox

The Sandbox Bill is aimed at facilitating financial innovation by providing a controlled space (“**Sandbox**”) where projects and tests in respect of such projects may be performed in a controlled and limited manner, provided that such technology-based projects are sufficiently developed to be subject to testing.

Such innovative projects must have an added value in at least one of the following aspects:

- The performance of regulatory compliance.
- Benefitting the users of financial services either in the quality of the service, the access to the service, the improvement of the type of services or the protection to the customers.
- Increasing the benefit for the entities or for the markets.
- Providing for mechanisms that improve regulation or the performance of regulatory supervision.

The Sandbox Bill does not restrict its scope to certain operators and, consequently, both new independent Fintech entities and incumbent players in the market may be admitted, provided that the projects they present meet the legal requirements. Furthermore, it is even possible that the public authorities also file applications in respect of projects which are deemed of general interest.

Filing of applications

The sponsors of the project shall apply for access to the Sandbox by means of an application form that shall contain an explanatory memorandum where the proposed project shall be explained, and the fulfilment of the requirements under “Requirements to access the Sandbox” above shall be justified. The explanation of how the guarantee system required shall be complied with will also need to be provided. Applications shall be made to the Treasury and International Finance Secretariat (the “TIFS”).

The Sandbox Bill provides for half-year cohorts, and, consequently, the deadline for admissions shall be fixed on a semi-annual basis.

Preliminary assessment

Within a month of the expiry of the term of admissions, the competent supervisors (BoSp, CNMV and/or GDI) shall make an assessment on the relevant applications and deliver them to the TIFS. A commission appointed within the TIFS shall acknowledge the projects with a preliminary favourable assessment and shall publish the list of such projects.

Test protocol and performance of tests

The sponsor and the relevant supervisor shall enter into a test protocol in respect of the project that will include, among others, the time and volumes of the tests to be performed, the information to be provided to the authorities, the phases and goals of such tests, the resources required by the sponsor to perform the tests scheduled and the guarantee scheme to be provided by the sponsor.

All participants in the test must sign an informative document whereby they shall provide the contents of the tests, the existing risk and the possibility to withdraw from the test. The document shall also contain a specific data protection clause.

The sponsor shall be liable *vis-à-vis* the participants of the damages suffered by the latter as a consequence of the tests. The sponsor shall not be liable from damages resulting from price fluctuations in the terms foreseen in the protocol.

The sponsors must offer a guarantee scheme which needs to be described in the protocol in order to cover the possible liability resulting from the damages they may incur while performing the tests. Such guarantee scheme may consist of insurances, performance bonds or guarantees.

Tests are to be finalised within six months, although this initial period may be extended by up to six additional months.

Monitoring

The regulator shall designate one or more monitors that shall supervise the tests. If there is more than one supervisor involved, each of them shall appoint a monitor.

During the performance of the tests, continuing communications between the supervisory authority and the sponsor will take place, and the supervisor shall be entitled to issue indications in order to comply with the protocol or the applicable laws. Likewise, the supervisor shall be entitled to request amendments to the protocol that may improve the performance of the tests.

The supervisor shall be entitled to demand any information or make the inspections they deem convenient.

The sector has raised the concern that it is key to the success of the Sandbox to allocate the required resources, including a reasonable number of trained professionals, who will act as monitors.

Suspension, conclusion and termination of the tests

The tests may be concluded at the request of the sponsor:

- If the targets of such tests have been achieved.
- For technical reasons or any other reason that may prevent their continuation. The Sandbox Bill also provides for the possibility to suspend such tests.

The supervisors may also suspend or terminate the tests in the following circumstances:

- Failure to comply with the applicable provisions of the protocol, the Sandbox Act or the best financial practices.
- Manifest deficiencies in the project.
- Existence of risks for the financial markets, financial stability or the protection of the clientele.

Assessment of the result and access to the activity

After the tests have been finalised, a memorandum assessing the results of such test and those of the project as a whole shall be prepared.

Once the project has been finalised, or even at an earlier stage if so provided in the protocol, the sponsor may request the authorisation to commence the activity or to extend its existing authorisation to the new activity that was the subject of the project.

The supervisory authorities in charge of the authorisation of the activity may deem that, as a result of the tests performed, a simplified procedure to authorise the activity may be used. This simplified procedure will cause the term given to the supervisor to grant any required authorisation for the performance of the tested activity to be reduced by half of its regular duration. The authorities may also waive any requirement for the authorisation that may have been evidenced to them in the course of the tests.

While this reduction in the regular terms has been viewed very favourably by the Fintech sector, it should be noted that, as a matter of fact, the authorities that are in charge of granting the relevant authorisations for the performance of activities in the financial sector generally exceed the terms provided by law to grant such authorisations. This generally occurs as a result of requests for additional information or amendments in the documents presented to the authorities. Halving the periods to grant any authorisation will thus have a limited use unless accompanied by certain changes in the operative functions of the supervisors. In addition to this, the Sandbox Bill does not provide for a transitional limited licence for the sponsors to operate while the authorisation is obtained. This may cause severe disruption in the operative functions of the sponsor, who will be forced to shut down its activities while the authorisation process is ongoing.

The Sandbox Bill also provides for the use of the proportionality principle in order to assess the fulfilment of the requirements to obtain authorisations by the sponsors, and the possibility to waive certain requirements within the limits permitted by Spanish law. The reach of this provision, should the Sandbox Bill be finally enacted, is yet to be seen, since no discrimination would be possible with incumbent players and the real possibility granted by law to waive existing requirements is very limited under Spanish law.

Restrictions

Since most activities were regulated prior to the surge of the Fintech sector, the existing regulations were created for a very different type of operator, who would normally be bigger, less focused on technology and would offer a relatively wide variety of services to their clients rather than specialising in certain specific services. This, in addition to the limits that have been pointed out in respect to each vertical, causes certain *de facto* restrictions, which include:

- (i) *Minimum capital requirements and full disbursement.* The minimum capital requirement varies significantly depending on the precise entity that would need to be incorporated and authorised to render the service. Investment services entities rendering services that may qualify as advice may require only €50,000, whereas a bank would be required to have a fully paid share capital of at least €18 million. The requirement of having the share capital fully paid in as from day one in most activities has also been viewed as a hurdle to the development of the sector.
- (ii) *Organisational requirements.* The same organisational requirements that need to be fulfilled apply to each investment service entity, irrespective of the activities it performs, with very few regulatory exceptions (such as the Simplified Securities Agencies, which have less requirements and may only perform the activity of conveying transaction orders from their clients). It has been proposed that simplified regulations for entities performing only specific activities should be enacted.
- (iii) *Lengthy authorisation processes.* As outlined above, the processes to obtain the required authorisations in Spain are very long, especially as a result of the common practice existing to date of requiring additional information and/or amendments to the documents filed, which cause the procedure to be extended over the maximum statutory periods.

Crypto-assets

In Spain, no laws or regulations have been issued as regards crypto-assets. As of today, only certain pieces of guidance issued by the CNMV (in some cases, jointly with the BoSp and other authorities) exist. The resulting legal uncertainty causes significant hurdles to the development of this vertical.

The main aspects that have been brought to the attention of the regulator are the following:

- (i) The fact that crypto-assets may meet the requirements to be considered securities and, thus, could be subject to the securities issues and markets regulations. As a result of this, those crypto-assets that qualify as “security tokens” shall be subject to the securities markets regulations, whereas those qualifying as “utility tokens” shall not.

The CNMV has issued two communications (dated 8 February 2018 and 20 September 2018). Pursuant to the latter, a token will qualify as security if it is offered making explicit reference to the expectation of obtaining a benefit by the purchaser as a consequence of its revalorisation, or a remuneration associated to the token, or mentioning the possibility to be negotiated in markets similar to regulated ones. However, if there is not a reasonable correlation between the expectation of revalorisation and the evolution of the underlying project, the token shall be deemed a utility token.

- (ii) The role of investment services companies in respect of issues of security tokens which qualify for partial exemptions for the application of issues and stock market regulations.
- (iii) The issues that arise as a result of their particular form of representation, and the fact that Spanish securities markets require certain specific forms of representation of securities which do not include blockchain technologies.

- (iv) The fact that the high risk and the very specific characteristics of such assets need to be brought to the attention of the public. The general view of the authorities – both domestic and in many countries of a similar economic environment – is that crypto-assets are unsuitable for retail investors.
- (v) The existing limitations as regards collective investment schemes that may invest in crypto-assets. According to the CNMV, only closed-end funds are suitable for such type of investment. This sort of funds may only sell stakes or shares in them to professional investors.
- (vi) The fact that, although trading platforms are not regulated in Spain – so long as the crypto-assets being traded are not considered securities – they should voluntarily apply certain principles governing the securities markets generally in a voluntary manner. In this regard, it should be noted that until Directive (EU) 2018/843 is transposed, exchanges are not affected by the anti-money laundering regulations, although banks and other entities used to make payments today in fiat currency are indeed affected. The transposition of EU Directive 2018/843 will cause that both exchanges and wallet service providers become subject to the anti-money laundering regulations.

Cross-border business

Spain is a heavily banking-based jurisdiction. This is mainly due to historical reasons (the development of the stock markets occurred only in the late 80s), the full-service approach of the credit institutions and the possibility that they have to obtain from the CNMV the required authorisations to provide investment services. In these circumstances, as of today, the impact of Fintechs and their disruptive approaches, while increasingly important, is still limited (according to sector sources, less than 5% of the European investment in Fintech in Q1 was performed in Spain. The UK exceeded 38%, and Germany 29%).

Spanish Fintechs generally view the following countries as the best for escalating their businesses:

1. Mexico.
2. Portugal.
3. Colombia.
4. Chile.
5. Germany.

Sector organisations, such as the Spanish Fintech and Insurtech Association (*Asociación Española de Fintec e Insurtech*) (“**AEFI**”), have developed close ties with its Latin American equivalents.

The CNMV has entered into a significant number of agreements with the regulators of other countries, which mostly relate to exchange of information in order to coordinate inspection activities, but the Fintech sector has not been subject to a specific approach as of yet. This reality is coherent with the state of development of the Fintech regulation in Spain.

**Guillermo Yuste de Ayala****Tel: +34 663 329 645 / Email: guillermo.yuste@andersentaxlegal.es**

Guillermo Yuste is a Partner in the Corporate Department at the Madrid office of Andersen Tax & Legal.

Previously, Guillermo Yuste was a Partner of Araoz & Rueda, heading the Banking and Finance Department of the firm, and he was an Associate at Linklaters.

Guillermo Yuste is a specialist in Banking and Finance Law and he has wide experience in cross-border financial transactions, trade financing, syndicated financing, acquisition financing, project finance related to renewable energies, as well as regulatory matters, debt restructuring, insolvency, aircraft financing and credit portfolio purchases. He also specialises in blockchain and Fintech regulation.

His experience in Banking and Financial Law has also been recognised by relevant legal directories such as *Chambers & Partners*.

Andersen Tax & Legal Iberia, S.L.P.

Velázquez, 108-110, 28006 Madrid, Spain
Tel: +34 917 813 300 / URL: www.andersentaxlegal.es

Sweden

David Frydlinger & Caroline Olstedt Carlström
Cirio Law Firm

Approaches and developments

Sweden is one of the most advanced fintech countries in the European Union, and possibly the world. Sweden is in general a highly digitalised country, not least in the traditional banking sector. The European Commission has, for instance, been monitoring Member States' digital competitiveness with the Digital Economy and Society Index (DESI) reports since 2015. The DESI 2019 report, published in mid-June, shows, for instance, that Sweden holds a steady second place in Europe with regards to digitalisation. The OECD has also in reports declared Sweden to be one of the leading countries in digital innovation.

Almost all Swedes are regular or frequent internet users, with only a few per cent never being online.

Swedish businesses embrace new technologies, such as cloud services, and every third SME sells online. Ten per cent of turnover comes from online sales.

Sweden is moving towards being a cashless society, where most transactions are carried out using credit or debit cards or other digital payment solutions. Furthermore, both businesses and consumers have for many years had steadily increasing access to digital banking services, regarding bank accounts, payments, trading, lending, financing and other services. All of the dominating Swedish banks offer not only internet banking via web interfaces, but also rather advanced apps, making it possible to handle a large number of bank-related matters via a smartphone. Also, attempts are being made to use robo-advisors. The number of physical bank offices are, consequently, steadily decreasing.

This strong digitalisation of the financial sector has been partly driven by challenges from fintech challengers and successful disruptors, but also to a large extent by the dominant players themselves, the incumbents. There is here an interesting interaction between the traditional large Swedish banks and challenging fintech players, with a combination of head-on competition and collaboration. One reason for this is of course that Sweden very early saw several disruptors in this industry, and fintech has since then become a mature market. Most banks have used a mixed strategy of in-house development of digital offerings and licensing of solutions from fintech companies, often combined with direct investments in these companies. Other important factors enabling strong digitalisation is the general access in Sweden to solutions for electronic identification.

Electronic identification is something that early on was considered as solved in the Swedish market, thanks, of course, to technical innovations, but also based on the fact that all Swedes are easily identified via their Swedish personal identity number. The personal identity number consists of the date of birth and with four additional digits attached to it (YYMMDD-XXXX). It is obtained when a person is entered in the Swedish population register by the

Swedish Tax Agency. It is widely used for everyday purposes in Swedish society, such as setting up memberships and subscriptions and to establish, for instance, a banking relationship with a Swedish bank, enabling online payments, etc.

Furthermore, Sweden is an open society with a generally high degree of consumer trust in service providers. The financial services and the incumbent banks especially enjoy a high degree of trust by customers (consumers as well as businesses). A combination of easy access to efficient online identification mechanisms and the Swedish trust in digital services led early on to easy access to trustworthy data sources in Sweden, enabling efficient online identification methods and forming a good basis for efficient know-your-customer assessments, credit assessments and fraud prevention.

As a result of the above, Swedish customers have broad access from both traditional banks and fintech companies to digital solutions, such as account information services, payment initiation services (where, for example, apps can be used to initiate payments from the customers' bank accounts), trading platforms, lending platforms, crowdsourcing and peer-to-peer platforms, and so on.

Interestingly, the strong development described above has largely taken place without regard or support of a regulatory framework. EU Directive 2015/2366 on payment services – commonly referred to as “PSD2” – will be implemented into Swedish law in September 2019, forcing the traditional banks to open up their databases via standardised interfaces. But this will happen at a time where Swedish customers already have access to the solutions which the PSD2 is supposed to enable. What impact the implementation of the PSD2 will have on the Swedish fintech market, if any, is yet to be seen. Naturally, the EU General Data Protection Regulation (GDPR) has had important consequences for the fintech sector, but since the level of compliance is generally high, the GDPR has not restricted the growth of the Swedish fintech market.

Sweden still waits, however, to see a strong uptake in blockchain-based solutions, such as cryptocurrencies. There are a number of reasons behind this, not least the large transaction costs of implementing such solutions involving many players, but one of them has been a still existing regulatory uncertainty as to the permissibility of the use of cryptocurrencies.

Fintech offering in Sweden

As described in the previous section, Swedish customers – both consumers and business customers – have access to a wide variety of fintech offerings. The most important categories of such services are described below.

Personal financial management, where consumers can get access to aggregated account information about their financial situation from all their banks and similar institutions. These services may also include payment initiation, fraud detection, lending services and similar services.

Payments, where paying customers as well as merchants are provided with alternative solutions for payments both on the internet and in retail stores.

Lending, where customers can borrow, and investors also invest money for lending, via platforms not connected to the traditional banks.

Trading platforms, providing customers with portfolio management services for stocks and funds.

Banking services, providing customers with a full set of services traditionally provided by the large Swedish or Nordic banks, including account management, lending and payments.

As already stated above, these and other services have evolved within the existing legal and regulatory framework, without specific support from, for example, the national implementation of the PSD2. This development has thus been driven by technology and access to funding from investors.

Regulatory and insurance technology

During recent years, Sweden has seen the establishment and growth of a number of regtech companies, but market development is still in an early stage. There are a number of companies providing solutions for compliance with the GDPR, including personal data records, data privacy impact assessments, incident management, etc. In addition, there are a growing number of companies offering solutions for anti-money laundering management – not least know-your-customer (KYC) checks – and insider information management.

There is also an ongoing clear uptake of progressive technologies in the insurance industry, including machine learning, artificial intelligence, and robot process automation to increase efficiency in claims processes. This development is mainly taking place within large insurance companies and, as of yet, Sweden has yet to see the growth of an insurtech industry.

Regulatory bodies

The following are the most important regulatory bodies for Fintech in Sweden:

The Financial Supervisory Authority, which authorises, supervises and monitors all companies operating in Swedish financial markets, including banks and other credit institutions, securities management companies, stock exchanges, and insurance companies.

The Data Protection Authority, which supervises and monitors compliance with the GDPR.

The Consumer Agency, which safeguards consumer interests, not least by monitoring compliance with consumer legislation.

Key regulations and regulatory approaches

The Swedish financial sector is highly regulated. Being a Member State of the European Union, the key regulations in Sweden are largely based on European Union regulations and directives. While this is the case, it is also important to note that the growth of the Swedish fintech sector has played out largely independent of laws and regulations, or rather within a legal framework not necessarily adapted to the new market environment for financial services.

There is no general regulatory approach to regulation of fintech activities in Sweden. Also, there is not only one or a few laws, but instead a multitude of laws, which become applicable depending on the activities carried out.

As regards regulations specific to the financial sector, there are three broad categories of laws and regulations: (i) laws regarding banks and credit institutions; (ii) laws regarding insurance and related activities; and (iii) laws regarding trade of securities. Depending on the activities of the specific fintech company, laws from one or all three of these categories can become applicable.

Banks and credit institutions are subject to various rules, of which the **Banking and Financing Business Act (2004:297)** is the most important. A typical fintech company

would, however, not apply for a licence to carry out banking activities, so this law would rarely be applicable.

In the current state of the Swedish fintech market, a law of particular importance is the **Act (2010:751) on Payment Services**, which also includes the main body of the implemented PSD2. The Act applies to payment services being provided in Sweden, and also to account information services and payment initiation services. Providing such services requires a licence from the Swedish Financial Supervisory Authority; however, certain exceptions exist for account information services. To obtain a licence, the company must show that the company management, as well as persons with significant influence in the company through share ownership or otherwise, have the necessary qualifications, knowledge and insight to run the business, and that necessary insurance coverage exists. For companies holding a licence, there are also additional requirements for minimum funding.

Furthermore, the Act on Payment Services includes rules regarding what is commonly referred to as “open banking”. Under these rules, banks and other financial institutions are obliged to provide third parties with access to payment systems and payment account services, enabling such third parties to, for example, establish personal finance management services. As from September 2019, banks and other institutions will have to comply with the Regulatory Technical Standards issued by the European Banking Authority regarding the technical requirements for the interfaces giving third parties access to data.

For certain fintech offerings, the **Act (2003: 862) on Financial Advice to Consumers** will become applicable. The Act sets out rules for companies providing advice to consumers about placements of their financial assets.

In addition to sector-specific laws, there are a number of laws which have general applicability in the Swedish market, but which are highly relevant for the fintech sector. The most important of those laws is the European **GDPR**, which sets out the rules for the processing of personal data. Given the nature of the fintech business, the GDPR is a key regulation that every fintech player must take into consideration. The regulation requires, *inter alia*, data controllers – entities deciding the purpose and means of the processing of personal data – to only process personal data lawfully, fairly and in a transparent manner, for specified, explicit and legitimate purposes, to not process more data than what is necessary for the stated purposes, to ensure the accuracy of the personal data, to not store personal data longer than what is necessary for the stated purpose, and to ensure the confidentiality and integrity of the personal data.

For fintech companies providing lending services to consumers, the **Act (2010:1846) on Consumer Credits** will typically become applicable. The Act sets out mandatory rules regarding the offering of consumer credits. The Act contains rules about information requirements to consumers, restrictions on marketing, credit assessments, restrictions on changes of interest rates and other related rules.

A law of great practical importance for consumer-oriented fintech activities is the **Act (1994:1512) on Unfair Contract Terms in Consumer Contracts**, implementing European Union Council Directive 93/13/EEC on unfair terms in consumer contracts. The Act includes rules under which the Swedish Market Court may prohibit companies from applying unfair terms and conditions in their consumer contracts. Examples of unfair clauses are all clauses giving the company the discretionary right to alter prices, fees and other terms, limitations of liability, and formal requirements for terminating the contract.

The Financial Supervisory Authority works closely with the European Banking Authority in several matters, not least regarding regulation of the fintech sector. The Financial

Supervisory Authority has also initiated an innovation forum for the Swedish fintech sector. It is not a regulatory sandbox, but instead a meeting forum for the FSA and the various players in the market with the main purpose to share experience and views. The FSA's intention is to stay close to the development of the Swedish fintech market, with the dual purpose of monitoring compliance and enabling growth.

Restrictions

Apart from the general requirements to comply with applicable laws and regulation, there are no restrictions on fintech activities in Sweden.

It may be worth mentioning, however, that there are some regulatory obstacles that generally are perceived to sometimes prevent the proper scale-up that fintechs normally strive to achieve, of which could be mentioned:

Cloud matters: In March 2018, the US adopted the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") to enable US government authorities to acquire data stored by communication and cloud services both within and outside of the US. The primary effect of the CLOUD Act is that it extends the geographical scope of existing US legislation, thereby letting US authorities require service providers to grant access to data regardless of where the data is stored and whether it is stored by a US company or a foreign affiliate. However, the CLOUD Act also establishes a framework under which the US can conclude executive agreements with "qualifying foreign governments" to facilitate access to data stored with service providers.

There is a potential conflict between the CLOUD Act, the GDPR and potentially also other national legislation. Swedish policy is not yet clear on the consequences of this conflict, and the requirements have not yet been assessed in the Swedish court. The Swedish Financial Supervisory has struggled to embrace cloud services in outsourced financial operations in general (considering any use of cloud service infrastructure as outsourcing), but has in recent years, as mentioned, initiated an innovation forum for the Swedish fintech sector. This entails a great development for the fintech sector and forms a basis for good progress in this area.

When considering cloud services in general, and especially if potentially impacted by the CLOUD Act, it is therefore important for a Swedish fintech to properly identify and assess the risks, also considering the US implications of the Act.

Fraud prevention: Under the previous European data protection directive and its national implementation in Swedish law (Swedish Personal Data Act), the prohibition on processing personal data concerning legal offences was interpreted both by the Data Protection Authority as well as Swedish courts to have a very wide scope, including also a prohibition on data controllers other than the public authorities to process even their suspicion of any such legal offences. This led, for instance, to fraud assessments and fighting criminal activities in general by digital means being a challenge for Swedish data controllers.

The prohibition on processing personal data relating to criminal convictions and offences according to article 10 has been considered by the Swedish Data Protection Authority as still also embracing the processing of personal data relating to suspicion of such criminal activities.

It remains to be seen if the scope of the prohibition under the GDPR would be considered as wide by the courts today post-GDPR. For now, the Swedish authorities are still requiring Swedish data controllers to submit applications for exemption from the prohibition in order

to be able to, for instance, screen prospective and current customers and their representatives against the US's so-called OFAC lists (the lists of economic sanctions against individuals and entities published by the US Treasury Department, Office of Foreign Asset Control). Such screening is an important part of international business today, and if such an application is dismissed, or not submitted, it would place a fintech company in a difficult position, with their business affected negatively since fulfilling legal requirements under US sanctions law would be made impossible; and thus the company would be put in a less favourable position than competitors in other countries. That could in turn lead to discontinued business relationships, partnerships that cannot be realised, the risk of penalties from US authorities and difficulties to compete.

Cross-border business

Business and consumer fintech customers are still mostly being provided with services from Swedish fintech companies. During recent years, however, there has been a growth in foreign investments in Swedish companies, such as Ingenico's acquisition of Bambora and PayPal's acquisition of iZettle. A growing number of Swedish fintech companies have also started to expand their business abroad, notably Klarna Bank. This growth of cross-border business calls for harmonised rules, which are also largely provided by the regulations and directives of the European Union.

**David Frydlinger****Tel: + 46 766 17 09 85 / Email: david.frydlinger@cirio.se**

David is managing partner of Cirio and also head of Cirio's digital offering. He has large experience in advising small, medium and large Swedish and international companies on digital matters, not least in the fintech sector. His advice includes regulatory advice on data privacy, financial regulation, consumer laws and contract drafting and negotiations.

**Caroline Olstedt Carlström****Tel: + 46 703 53 90 30 / Email: caroline.olstedt.carlstrom@cirio.se**

Caroline has 18+ years of experience in international data privacy and has served as legal/strategic advisor to companies within IT, media, telecommunications, and finance sectors. She served for five years as Vice President of Privacy at Klarna Bank with global responsibility for Klarna Group's data protection strategy and compliance and managing its Global Privacy Office. Today she is a partner at Cirio, responsible for Cirio's Data Privacy & Information Security Practice, and still working with Klarna Bank, now as external Data Protection Officer (DPO). Caroline is also appointed as external DPO for Nasdaq's regulated businesses in the Nordics and Baltics. Caroline is chairman of the Swedish Data Protection Forum and involved in several industry data privacy taskforces, such as, for instance, the Swedish ICC's Policy Commission for Digital Economy.

Cirio Law Firm

Mäster Samuelsgatan 20, PO Box 3294, 103 65 Stockholm, Sweden

Tel: +46 852 79 16 00/ URL: www.cirio.se

Switzerland

Lukas Morscher, Fedor Poskriakov & Isy Isaac Sakkal
Lenz & Staehelin

Approaches and developments

The market conditions in Switzerland for Fintech offerings are generally considered as favourable, in particular based on broad access to credit and venture capital, the available human know-how (number of graduates in science and technology), as well as the access to, and use of, information and communication technology. The Fintech market growth (value chain share) and expansion (range of products and services) have accelerated in Switzerland based on an already relatively high level. In 2018, the total amount of money invested in the Fintech industry rose sharply by 61.8%, compared to the previous year, to reach 75.7 million Swiss francs, with a high number of financing rounds raising over 3 million Swiss francs.¹ For the Fintech industry, the decisive considerations remain in financing and fundraising.

The Swiss Fintech landscape has evolved significantly over the past few years. Switzerland remains an attractive base for innovators in the financial sector. There are currently more than 200 active players (both emerging and incumbent) in Switzerland's Fintech ecosystem, whilst the total number of Fintech-related businesses is much higher. Most of their business models focus on the financial market sector (notably payment services, investment management, banking infrastructure, deposit and lending, distributed ledger technology (DLT) and analytics). A considerable number of these businesses offer their products and services to incumbent financial institutions and/or offer cooperation opportunities with respect to digitalisation projects.

Overall, the Fintech market in Switzerland is dominated by start-ups that are mainly financed through venture capital. A cooperation strategy between established providers of financial services and emerging players is common in Switzerland. While no general displacement trends can be identified at present, it is apparent that the value chain of established providers of financial services is under scrutiny and subject to (internal and/or external) challenges, including based on technology-driven new products and services developed by emerging companies that have the potential to disrupt the value chain of many established players. Established financial service providers generally have the financial and organisational resources required to adapt their business processes gradually to avoid such displacement and get high market visibility. Conversely, only a relatively small number of emerging companies can rely on a trust-emanating brand or a financial market licence (e.g., as a bank or a securities dealer).

Various associations and interest groups have been set up to coordinate the interests of Fintech-oriented organisations and individuals. They organise networking events, facilitate the exchange of experience and know-how and raise the voice of the Fintech sector in politics. In addition, the federally funded Commission for Technology and Innovation provides

financial and administrative support (subject to certain eligibility criteria). Furthermore, a considerable number of private initiative incubators and accelerators are active or have been recently launched to support emerging Fintech companies in the development of their business ideas and models. A number of Fintech-specific awards and challenges (e.g., Swiss Fintech Awards) are also intended to encourage innovation in the Fintech sector.

Fintech offering in Switzerland

The most represented areas of Fintech include the following:

Robo-Advisors and high-frequency algorithmic trading

In Switzerland, financial advisors providing financial advice or investment management services online via automated or semi-automated systems, so-called “Robo-Advisors”, are growing in popularity. Several companies offer Robo-Advisor services aiming at allocating, managing and optimising clients’ assets based on mathematical rules or algorithms, which automatically determine the triggering and the individual parameters of an order (such as time, price or quantity). High-frequency trading is a subcase of algorithmic trading with very low delays in order generation and transmission, which usually pursues a very short-term trading strategy. Its distinctive feature is a high number of order entries, changes or deletions within microseconds.

Crowdlending

Crowdlending refers to alternative ways of raising capital from many participants using online platforms with or without professional intermediaries. Crowdlending is also known as peer-to-peer (P2P) or social lending because funding is provided by individuals or companies that are not financial institutions or intermediaries. Participants (funding providers) typically receive a payment in return for their funding made available to the project developer (borrower) in the form of interest, although participating loans or bonds/notes issuances are also possible. The amount of the interest or return payment varies depending on the risk of the project and borrower, but generally represents a lower cost of funding for the borrower than traditional bank lending. There are a number of crowdlending-based platforms in Switzerland which offer loans for both private persons and companies. Currently, the Swiss regulatory framework for financial activities does not contain any specific rules regarding crowdlending activities (see below under “Key regulations and regulatory approaches”).

Payment processors

In Switzerland, the payment services market has evolved during the last few years. Since the first market entry of a mobile payment app, the Swiss market has seen several new companies and a rapid consolidation process. Many electronic payment systems are at least partially based on classic credit or debit card payment schemes, using technology to facilitate payments at the point of sale, in the context of e-commerce, or in some cases between individuals (P2P). In addition to credit and debit card-based payments, some payment apps may be linked to traditional bank accounts with partnering banks. While the user experience is similar, the payment is in this case executed as a bank transfer. These systems are often bank-operated or bank-sponsored, and may therefore be less constrained in regulatory matters.

Distributed ledger technology

DLT, such as various blockchain implementations, have been the focus of many public and private initiatives. Whilst the Swiss legislature is aware that the possibilities offered by

DLT/blockchain go far beyond the application to such alternative financings, there is currently a legislative focus on the financial sector. The Swiss Federal Council published in December 2018 a report on the legal framework for blockchain and DLT in the financial sector. The report noted that the Swiss legal framework is well suited to deal with new technologies, although a few selective adjustments are expected to be implemented in the coming years. Furthermore, traditional fundraising techniques and processes have been challenged in the last couple of years by the emergence of a new form of capital raising by start-ups in the form of initial coin offerings (ICOs) or token-generating events based on DLT technology. In this context, the Swiss Financial Market Supervisory Authority (FINMA) published the “ICO Guidelines for enquiries regarding the regulatory framework for initial coin offerings” on 16 February 2018. Generally, FINMA focuses on the economic function and purpose of the tokens, as well as whether they are tradeable or transferable, in order to classify the tokens broadly into three “archetypes”, which are payment tokens (which include cryptocurrencies), utility tokens or asset tokens. The classification of the tokens has an impact on the applicable legal and regulatory framework (see below under “Key regulations and regulatory approaches”).

Regulatory and insurance technology

The InsurTech market in Switzerland is growing rapidly, due to, for example, organisations pursuing business models which are based on the general challenges faced by incumbent insurance institutions (e.g., new regulatory frameworks, the inflow of alternative capital and the ongoing low interest rate environment). In general, incumbent insurance institutions have lower barriers when entering the InsureTech market, as they already have the corresponding licences and are able to focus on the development of the technology. To date, no legislation specifically refers to InsureTech business models. In this context, regulatory implications for specific InsureTech business models must be assessed under the ordinary principles governing the provision of insurance services, in particular as regards maintaining the protection objectives of insurance supervision by FINMA.

RegTech is a subset of Fintech focusing on technologies that may facilitate the delivery of regulatory requirements in a cost-effective and comprehensive way. RegTech refers to technology and software created to address regulatory requirements and help companies stay compliant, including by leveraging software and automation to close compliance gaps and to monitor and detect risks on a permanent basis. Outsourced functions by financial institutions (e.g., operational risk management and compliance tasks) is an important segment for RegTech companies. Again, to date, there is no legislation specifically referring to RegTech. FINMA has generally been welcoming technology applications supporting supervised entities in complying with regulatory requirements. Conversely, however, there are no material efforts led by the Swiss regulator to promote the development, use and reliance of technology for regulatory compliance, despite the fact that FINMA has adopted a number of initiatives to digitalise its own processes (e.g., electronic data reporting, only secure document filing and transmission platform, etc.).

Regulatory bodies

In Switzerland, the legal framework governing the activities of Fintech operators consists of a number of federal acts and implementing ordinances issued by the Federal Council. The Swiss legal and regulatory framework does not foresee a single authority responsible for the overall supervision of Fintech companies. In this context, the following regulatory bodies and authorities may be involved depending upon the type of legislation concerned.

FINMA

FINMA is Switzerland's regulator supervising the financial markets and its participants. The applicable licensing requirements or special approval processes, if any, depend on the business model of any given Fintech company. FINMA's regulatory powers are derived from the Federal Act on the Swiss Financial Market Supervisory Authority (FINMASA). Generally speaking, FINMA is responsible for the authorisation, supervision, enforcement and documentation of all activities that require an approval. The supervision is risk-based depending upon the respective financial market participant. Financial market laws are enforced by FINMA, making use of administrative measures where necessary. FINMA is also competent to issue implementing ordinances as well as circulars and other guidance. As regards Fintech in particular, FINMA intends to strengthen Switzerland's position as one of the leaders in this sector. As a result, in 2016, FINMA put in place a specific Fintech desk to address this sector's issues more efficiently.

Self-regulatory organisations (SROs)

Swiss Fintech companies that are financial intermediaries operating on a commercial basis are subject to the Swiss anti-money laundering framework, namely the Anti-Money Laundering Act (AMLA) (see below under "Key regulations and regulatory approaches"). Companies subject to AMLA that are not otherwise supervised by FINMA (e.g., a bank or securities dealer) must either hold a FINMA licence as a directly subordinated financial intermediary or become a member of a self-regulatory organisation (SRO) recognised by FINMA. While having limited enforcement powers, SROs are responsible for supervising compliance with the due diligence obligations of the financial intermediaries. In turn, FINMA actively supervises the SROs.

Data Protection Commissioner

The Federal Data Protection and Information Commissioner (FDPIC) is the federal data protection authority in Switzerland. In addition, cantons are competent to establish their own data protection authorities for the supervision of data processing by cantonal and communal bodies. The FDPIC has no direct enforcement or sanctioning powers against private bodies processing personal data. Nevertheless, the FDPIC can carry out investigations on its own initiative or at the request of a third party (i) if methods of processing are capable of violating the privacy of a large number of persons (system errors), (ii) if a specific data collection must be registered, or (iii) if there is a duty to provide information in connection with a cross-border data transfer. To this effect, the FDPIC may request documents, make inquiries and attend data-processing demonstrations. On the basis of these investigations, the FDPIC may recommend that a certain method of data processing be changed or abandoned. Whilst these recommendations are not binding, if a recommendation made by the FDPIC is not complied with or is rejected, the FDPIC may refer the matter to the Federal Administrative Court for a decision. The draft of the revised Data Protection Act (DPA) foresees that the FDPIC will be able to issue binding administrative decisions (instead of recommendations under the current DPA); for example, to modify or terminate unlawful processing.

Criminal authorities

In addition to FINMA, which is competent to issue administrative sanctions, criminal prosecution authorities are also involved in enforcing financial market laws. Where irregularities fall under criminal law, FINMA may file a complaint with the competent authorities (Federal Department of Finance, Office of the Attorney General and cantonal prosecutors). As an example, the exercise of an activity that requires a licence under the financial markets legislation without having obtained said licence is a criminal offence.

Key regulations and regulatory approaches

Swiss law is generally technology-neutral and principle-based. Accordingly, Fintech companies based in Switzerland generally have considerable regulatory latitude compared to other jurisdictions. That being said, since 2015, the legislator's focus has been on adapting the applicable legal and regulatory framework to the needs of the Fintech sector. In this context, the Swiss legislator introduced three measures within Swiss banking legislation aiming at promoting innovation in the financial sector, i.e.:

- the introduction of a maximum period of 60 days (as opposed to seven days, in accordance with FINMA's prior practice) for the holding of monies on settlement accounts (e.g., for crowdfunding projects), without any limitation in terms of amounts;
- the creation of an innovation area called a "sandbox", where companies are allowed to accept public deposits up to a total amount of 1 million Swiss francs without the need to apply for a banking or fintech licence, subject to certain conditions such as disclosures and a prohibition to invest deposits; and
- the introduction of a new Fintech licence suitable for businesses whose activity involves some form of deposit-taking, but without any lending activities involving maturity transformation.

The first two measures of this so-called Fintech regime entered into force on 1 August 2017, whilst the Fintech licence entered into force on 1 January 2019, along with amendments to the Banking Ordinance adopted by the Swiss Federal Council on 30 November 2018.

Under the Fintech licence, financial services providers are allowed to accept public deposits provided that (i) the aggregate amount of deposits does not exceed 100 million Swiss francs, (ii) the deposits do not bear interest (or are not otherwise remunerated), and (iii) the deposits are not re-invested by the company (i.e., they are not used for on-lending purposes). This new Fintech licence involves less stringent regulatory requirements than a banking licence. Strict banking equity ratio requirements as well as the liquidity requirements do not apply. In addition, leaner minimal capital requirements apply. In this context, the minimum equity capital of companies benefitting from such a licence has to amount to 3% of the public funds (deposits) and must, in any case, reach a minimum of 300,000 Swiss francs. On 3 December 2018, FINMA issued guidelines for the Fintech licence, highlighting the information and documentation that an applicant must submit when applying for such licence. This namely includes a list of all participants holding a direct or indirect interest of 5% in the applicant, information on the governing bodies, as well as various explanations on the activities of the company with a business plan for three financial years. To be clear, the Fintech licence is not a banking licence, and companies operating under such a licence do not qualify as a banking institution and may not use such designation. In this context, the client deposits are not covered by the Swiss deposit protection regime and the clients must be comprehensively informed in advance of this fact, as well as of the risks resulting from the business model.

Alongside these specific Fintech-dedicated measures, the general applicable legal and regulatory framework applies to Fintech companies and may be summarised as follows:

Banking and securities-dealing legislation

The solicitation and acceptance of deposits from the public on a professional basis is, as a matter of principle, an activity restricted to Swiss banks and triggers the obligation to obtain a fully-fledged banking licence from FINMA. Under the Banking Act, the term "deposit" broadly encompasses any liability owed to a client. Deposits are deemed to be "public" as soon as (i) funds are solicited from the "public" (as opposed to being solicited from banks or

professional financial intermediaries, institutional investors/shareholders, employees or other related persons), or as soon as (ii) funds from more than 20 depositors are accepted. As a result of this approach, most business models relied upon by payment systems, payment services providers, crowdfunding or crowdlending platforms, for instance, are considered to involve the solicitation and acceptance of deposits and may fall within the scope of the Banking Act and, therefore, trigger licensing requirements.

That being said, in the event that deposits of not more than 1 million Swiss francs (see above “Sandbox” exception with applicable conditions) are held by a Fintech company, no banking licence will be needed. Similarly, if the deposits are held for less than 60 days on a settlement account (without any limitation in terms of amounts), no banking licence will be needed. All other deposit-taking activities require either a Fintech licence for a deposit-taking activity not exceeding 100 million Swiss francs, or a fully-fledged banking licence. It is also worth noting that funds linked to means of payment or to a payment system are exempted from the qualification as deposits, provided that (i) the funds serve the purpose of purchasing goods or services, (i) no interest is paid on them, and (ii) the funds remain below a threshold of 3,000 Swiss francs per customer *and* per issuer of a payment instrument or operator. Although this exemption may provide some relief to card payment services and online or mobile payment services, it requires a model strictly tailored in a way that any funds stored on user accounts be limited to the purchase of goods and services (as opposed to allowing peer-to-peer transfers, withdrawals, transfers to the user’s bank account, etc.) and never exceed 3,000 Swiss francs per customer.

Fintech companies may also fall under the scope of the Federal Stock Exchanges and Securities Trading Act (SESTA), as is generally the case for financial market infrastructures such as stock exchanges and multilateral trading systems. Companies buying or selling securities in a professional capacity on the secondary market, either for their own account with the intent of reselling them within a short time period, for the account of third parties, for making public offers of securities on the primary market, or offering derivatives to the public, also fall within the ambit of SESTA. In such case, a FINMA licence will be required.

Anti-money laundering legislation

Any Swiss-based natural or legal person accepting or holding deposit assets belonging to others, or assisting in the investment or transfer of such assets, qualifies as an intermediary according to AMLA. Namely, this includes persons carrying out credit transactions (in particular in relation to consumer loans or mortgages, factoring, commercial financing or financial leasing) or providing services related to payment transactions. This applies to many upcoming business models, such as those involving mobile payments, blockchain and related applications, cryptocurrencies, automated investment advice, crowdfunding or peer-to-peer lending. Based on this broad scope, many, if not most, Fintech companies qualify as financial intermediaries and are generally subject to anti-money laundering obligations, including compliance with know-your-customer (KYC) rules.

As mentioned, Fintech companies subject to AMLA are required to join a self-regulatory organisation or to obtain FINMA approval as directly supervised financial intermediaries (see above under “Regulatory bodies”). Compliance with Swiss anti-money laundering regulations is relatively straightforward and usually does not represent a significant entry barrier. However, dealing with the associated costs (which can be substantial and, hence, a key aspect with respect to certain business models) requires careful planning and possibly adaptation of envisioned business models. This applies, in particular, to Fintech companies providing alternative finance (e.g., crowdlending) platforms and payment services.

Similarly, compliance with AML/CFT requirements may be challenging for virtual currency payment products and services that rely on a set of decentralised cross-border virtual protocols and infrastructure elements. In this context, FINMA confirmed in its ICO Guidelines (see above under “Fintech offering in Switzerland”) that AML requirements may be fulfilled by having the funds accepted via a financial intermediary which is already subject to the AMLA in Switzerland, and which performs the corresponding due diligence requirements on behalf of the ICO organiser. In such circumstances, the ICO organiser does not itself have to be affiliated to an SRO or to be licensed directly by FINMA. Separately, FINMA also issued a circular on video and online identification (Circular 2016/7). Aimed at levelling the playing field and fostering technological developments, this circular provides for the possibility of financial intermediaries to comply with their KYC requirements by means of video transmission and other forms of online identification.

Data protection

The processing of personal data by private persons and federal bodies is regulated in particular by the DPA and the Data Protection Ordinance (DPO), which apply, with some exceptions, to the processing of data relating to natural persons as well as (contrary to most other jurisdictions) legal entities. Personal data must be protected against unauthorised processing by appropriate technical and organisational measures. Such protection has been specified with respect to the storing, processing and transferring of client data in the banking sector (Annex 3 to FINMA Circular 2008/21 on capital adequacy requirements for operational risks within the banking sector). Of note, Swiss data protection law is currently being amended. While the technical requirements are likely to remain unchanged, there are considerable organisational and administrative requirements as well as significant sanctions foreseen. However, the particulars of the amendments and the timeline with respect to the entering into force of such amendments are not yet determined.

As regards cybersecurity, non-binding guidelines with respect to minimum security requirements for telecommunications services have been issued by the competent regulator, the Federal Office of Communications (OFCOM). However, there is no cross-sector cybersecurity legislation in Switzerland that would generally be applicable to Fintech companies.

As regards blockchain, although the data stored on a public blockchain is usually encrypted, personal data can still be generated by linking further information enabling it to be assigned to a natural person. If this is the case, the transparency and immutability of the information documented on the blockchain are not compatible with the basic principles of data protection. Participation in a blockchain platform would, to some extent, be tantamount to giving up informational self-determination (consent) as the data has been entered voluntarily into the system. While encryption technology and digital signatures fundamentally increase data security, effective protection against loss or theft also depends, to a large extent, on the management of private keys. For example, several of the major thefts of tokens can be traced back to the improper management of private keys. For this reason, great importance must be attached to the safekeeping of private keys.

Other relevant legislation

Other legislation may apply to Fintech companies. As an example, under the Swiss Consumer Credit Act (CCA), only authorised lenders are entitled to provide consumer credits. Registration must be obtained from the lender’s Swiss Canton of establishment or, if the activity is conducted on a cross-border basis by a foreign lender, with the Swiss Canton in which the lender intends to perform its services. In the course of the amendment of the

Banking Act to introduce the new Fintech licence category (see above), the CCA has been amended. In this context, consumer loans that are obtained through a crowdlending platform will need to comply with the same consumer protection afforded by the law as if they were extended by a professional lender.

In addition, further licensing and supervisory requirements from the Swiss National Bank may be required for payment systems with payment settlement levels in excess of 25 billion Swiss francs (gross) per financial year, as well as for Swiss and foreign payment systems that are classified as “systemically relevant”.

Outlook

On 22 March 2019, following the Swiss Federal Council’s report on the legal framework for blockchain/DLT in the financial sector (see above under “Fintech offering in Switzerland”), the Federal Council initiated a consultation process on the adaptation of federal law to developments in DLT. With this proposal, the Federal Council plans to increase legal certainty by removing hurdles for DLT-based applications and limiting risks of misuse. The consultation process will last until the end of June 2019. In a nutshell, the legislative amendments considered include (i) a civil law change aimed at increasing the legal certainty in the transfer of DLT-based assets, (ii) the possibility of segregation of crypto-based assets in the event of bankruptcy, and (iii) a new authorisation category for DLT trading facilities which is intended for services in the areas of trading, clearing, settlement and custody with DLT-based assets. Overall, these legislative amendments are expected to increase market access to Fintech companies in the field of DLT/blockchain technologies by improving legal certainty and removing certain regulatory barriers.

In addition, the new Swiss Financial Services Act (FinSA) and Swiss Financial Institutions Act (FinIA) are expected to enter into force on 1 January 2020. Whilst the purpose of the FinIA is to provide a new legal framework governing most financial institutions (i.e., portfolio managers, trustees, managers of collective assets, fund management companies and securities firms), the objective of the FinSA is to regulate financial services in Switzerland, whether provided by a Swiss-based business or on a cross-border basis in Switzerland or to clients in Switzerland. The rules are largely based on the EU directives (MiFID II, Prospectus Directive, PRIIPs), with adjustments made to reflect specific Swiss circumstances. In a nutshell, as regards Fintech, the new legal framework may involve additional regulatory requirements to the extent that Fintech companies provide financial services in Switzerland, or to Swiss clients (application of FinSA), or provide asset management services or other regulated services (application of FinIA and new licensing requirements) (see also under “Cross-border business” below as regard cross-border regulation).

Generally speaking, the Swiss regulatory framework is expected to remain in a state of flux for the years to come, with changes aiming at promoting innovation in the financial sector while increasing client protection.

Restrictions

Based on its technology neutrality and principles-based approach, the Swiss regulatory framework allows for considerable regulatory latitude and room for development for Fintech companies. Two key principles of Swiss financial market regulation are system stability and consumer protection. Accordingly, a number of cross-sector regulations aim at strengthening the robustness of financial institutions while ensuring transparency. The specific Swiss Fintech regulation (see above under “Key regulations and regulatory

approaches”) maintains these principles while addressing the most critical barriers to innovative business models – i.e., the regulatory threshold for accepting client money and holding more than 20 deposits – and is tailored to allow fair and equal treatment of all market players while providing a risk-based framework to encourage innovation.

Traditional financial institutions encounter lower barriers when entering the Fintech market because such institutions are typically fully licensed and are, hence, in a position to develop and deploy technology-driven business models without the additional burden of ensuring that such development and deployment is in line with applicable general regulatory requirements. Several regulatory circulars and guidance papers, such as the FINMA Video and Online Identification Circular, FINMA ICO Guidelines and Swiss Federal Council’s report on the legal framework for blockchain/DLT in the financial sector are also aimed at lowering entry barriers for emerging companies by clarifying the regulatory framework applicable to Fintech companies. In this context, the current legal and regulatory framework generally allows new business opportunities for Fintech companies irrespective of the technology used, including by way of collaboration, outsourcing and otherwise.

In addition, it is worth noting that in the absence of international standards, FINMA, as well as other regulators across the world, generally adopt a cautious approach in relation to new technologies (e.g., capital adequacy requirements for cryptocurrencies). Such approach creates uncertainties for emerging Fintech companies as well as for existing financial institutions which are exposed to significant reputational risk.

Cross-border business

Currently, Swiss financial services regulation places a strong emphasis on the principle of “home country” control, and takes a liberal stance as regards the promotion and provision of financial services in Switzerland by financial service providers incorporated outside of Switzerland. As mentioned, such regime will shortly be impacted by the forthcoming overhaul of the regulatory framework applicable to the provision of financial services. New legislation is expected to enter into force on 1 January 2020 and will provide, *inter alia*, that a non-Swiss financial services provider acting on a cross-border basis will be subject to Swiss rules of conduct, as well as, under certain circumstances, registration requirements in Switzerland for its client advisors. Client advisors of foreign-based financial services providers will be required to register in a Client Advisors Register in Switzerland prior to being able to offer financial services or products in Switzerland. In this context, the registration requirement will not apply at the level of the financial services provider, but at the level of the individuals qualifying as “client advisors” of such financial services provider. A blanket exemption may end up being eventually granted to certain foreign-regulated institutions by the Federal Council.

As regards anti-money laundering obligations, the Swiss regime (AMLA) only applies to financial intermediaries that have a “physical presence” in Switzerland and, as a rule, does not extend to foreign institutions active on a pure cross-border basis. As an example, payment service providers conducting their activity exclusively via electronic channels or the Internet, for instance, are typically not subject to AMLA. That being said, irrespective of the application of AMLA, the general prohibition of money laundering under criminal law remains applicable.

Finally, it is worth noting that FINMA engages with a number of international bodies to establish a framework aimed at promoting innovation, as well as the protection of customers and investors in this area. In this context, FINMA has entered into several memoranda of

understanding with various foreign regulators and regularly cooperates with foreign regulators or organisations. As an example, FINMA entered into a cooperation agreement with the Monetary Authority of Singapore in September 2016 aiming at encouraging and enabling innovation in their respective financial services industries. Overall, both FINMA and the Swiss legislator endeavour to support financial innovation and to establish a Fintech-friendly environment.

* * *

Endnote

1. Swiss Venture Capital Report 2018, available at: <https://www.startupticker.ch/en/home>.

**Lukas Morscher****Tel: +41 58 450 80 00 / Email: lukas.morscher@lenzstaehelin.com**

Dr. Lukas Morscher is a partner and head of the TMT and Outsourcing practice in the Zurich office of Lenz & Staehelin and an expert on the digitisation of the financial services industry. He practises in transactional and regulatory matters, outsourcing (IT and business process transactions), TMT, internet and e-commerce, data privacy, Fintech and digitisation/industry 4.0. A member of SwissICT, the Swiss ICT association Swico and the International Technology Law Association (ITechLaw), Lukas Morscher is a frequent speaker on topics related to Fintech and digitisation.

**Fedor Poskriakov****Tel: +41 58 450 70 00 / Email: fedor.poskriakov@lenzstaehelin.com**

Fedor Poskriakov is a partner at Lenz & Staehelin in the Banking and Regulatory group in Geneva, and specialises in banking, securities and finance law. He regularly advises on various regulatory, contractual and corporate matters. His practice covers banking, investment management and alternative investments, including private equity and hedge funds. He also advises on complex asset structuring and protection for business and private assets. His other practice areas include compliance advisory, internal investigations, private clients and Fintech. Fedor Poskriakov is admitted to the Bar in Geneva. He has a law degree (*lic. iur.*) from the University of Geneva.

**Isy Isaac Sakkal****Tel: +41 58 450 70 00 / Email: isy.sakkal@lenzstaehelin.com**

Isy Isaac Sakkal is an associate in the Geneva office and is a member of the Banking and Finance group. His practice covers banking and finance, investment funds, Fintech, corporate, M&A and contracts. Isy Isaac Sakkal is admitted to the Bar in Geneva and New York. He has a Master's in Business Law from the University of Geneva (Switzerland), as well as an LL.M. degree from the University of California, Berkeley (USA).

Lenz & Staehelin

Route de Chêne 30, 1211 Geneva 6, Switzerland
Brandschenkestrasse 24, 8027 Zurich, Switzerland
Tel: +41 58 450 70 00 / +41 58 450 80 00 / URL: www.lenzstaehelin.com

United Kingdom

Ian Mason, Sushil Kuner & Samantha Holland
Gowling WLG

Approaches and developments

“FinTech” is the use of technology to facilitate financial services. The UK FinTech industry is reaching higher levels of investment than ever before, with well over £100 billion invested since the beginning of 2018. Such investment is changing conventional standards regarding investment, particularly as the majority of recent investments were driven by the investees rather than the investors. Investors for many years have been making equity investments in technology companies with high potential in the future, but now the market is beginning to see more businesses with sought-after products that are actively going to the market.

FinTech is also now drawing more innovative methods of investment. Particularly in the past few years, crowdfunding has been becoming a more established type of financing whereby individuals can invest in companies not listed on stock exchanges. This trend is likely to continue in the foreseeable future and we expect to see more companies that have gone through fundraising in this way making profitable returns to investors on exits, such as initial public offerings, share sales and asset sales.

The growth of the FinTech sector, together with evolutionary changes in the types of financial services, will also inevitably affect the composition of the UK jobs market. A small part of the workforce that consists of roles relating to technological creativity is expected to double in size within the next three years alone to reach just under one-third of the workforce.

One of the most interesting developments as a result of FinTech, however, will be the Uberisation of the UK financial services industry from its traditional UK home in the City of London. For example, Henri Murison, the Director of the Northern Powerhouse Partnership, has said that the future of Manchester’s economy will be heavily reliant on FinTech, particularly as it is fast becoming a major digital hub. Such activity will create great challenges for the City of London in wake of developments such as Brexit.

The UK FinTech offering

There are many key ways in which the technologies, applications and methods of financial services companies are disrupting traditional financial services markets. On an almost daily basis, we read headlines about blockchain and cryptocurrencies and their ability to speed up transactions. Permissioned blockchain, in which access is granted or prevented by those who administer it, has great potential. Several organisations are experimenting with such technology, particularly relating to digital currency payments. Smart contracts, which are also known as “programmable money”, have the ability to dramatically change transaction and insurance processes, by creating blocks based on conditions where transactions are executed provided that specified conditions are met.

Regulatory and insurance technology

RegTech

RegTech involves the use of technology to meet regulatory requirements in a more rapid and effective way than current systems. The use of automation and artificial intelligence (“AI”) can simplify standard processes, reducing cost and time involved. RegTech is a market “disruptor”, so has particular appeal to start-up and entrepreneurial tech companies as providers and suppliers, although established financial institutions (as well as regulators) are also very interested in RegTech.

There are already a number of established use cases for RegTech, and these are developing. European and UK anti-money laundering provisions require financial institutions (and others, such as law firms) to carry out identity verification and Know Your Customer (“KYC”) checks as part of customer due diligence (“CDD”) when taking on new clients. RegTech solutions can automate the verification to reduce the manual input required. The use of biometrics is also increasing in this area.

Regulatory reporting is another good use case for RegTech. Reporting typically involves submission of standardised returns to the regulator, with prescribed data fields. RegTech solutions can draw on multiple data sources and conduct automated searches far more quickly than using manual processes.

RegTech has also been used in customer-facing applications. A number of UK investment firms have launched “robo-advice” services, where customers answer standardised questions on their investment objectives and risk profile (among others), which inform the recommendation of an investment portfolio. The FCA has raised some regulatory concerns on pure auto advice services, and has emphasised that automated investment services must meet the same regulatory standards as traditional discretionary or advisory services.

However, one of the major uses of RegTech has been in the launch of Open Banking. This allows banks to provide access to customers’ data through third-party providers (“TPP”), using a secure application programme interface (“API”). Regulatory changes such as the implementation of the Payment Services Directive (“PSD 2”) have made this possible. There are at least 200 TPP firms authorised to operate in the UK, with another 130 going through the process. It is estimated that more than 7,500 new customers each day are sharing their data via Open Banking to aggregate their accounts.

The UK regulators have been keen to encourage innovation and the use of technology in financial services with the Financial Conduct Authority’s (“FCA”) Innovation Hub and Regulatory Sandbox (see below). The FCA is also one of the regulators involved in creating a global sandbox under the Global Financial Innovation Network (“GFIN”) (see below).

The FCA is considering how it can itself use RegTech. In the FCA’s Business Plan for 2019–20, it states that it will continue to explore how to improve the method of data exchange between industry and regulators, and specifically the opportunities for expressing these requirements in a machine-readable and executable form. The FCA will also look at delivering digital regulatory reporting in conjunction with the industry participants and the Bank of England.

InsurTech

A rise in InsurTechs and the increased use of technology by incumbent insurers has had a transformative effect on the UK insurance industry, impacting every aspect of the insurance value chain.

Smart devices and IoT have led to a rise in usage-based insurance, often on a peer-to-peer platform. Chat bots and machine learning are transforming sales and distribution channels. Big Data, telematics and AI allow for granular analysis of risk with more accurate pricing models, tailored products and a better customer experience. Distributed ledger technology (“**DLT**”) allows for greater efficiency in data-sharing, improved fraud detection and better regulatory compliance. Smart contracts are transforming claims handling with automatic pay-outs on the occurrence of an event without the policyholder ever having to make a claim.

In the UK, the insurance sector is regulated by the FCA whilst regulatory disputes between consumers and insurers or insurance intermediaries are determined by the Financial Ombudsman Service (“**FOS**”). The law on insurance contracts in England and Wales is principally governed by the Insurance Act 2015 (the “**Insurance Act**”) which is interpreted and applied by the English courts.

New insurance technology presents some legal and regulatory challenges:

- In the UK, an insurance contract is a contract of good faith and the Insurance Act sets out certain requirements around pre-contractual disclosure. An insured must give fair presentation of the risk but is not required to disclose information known to the insurer. The use of Big Data and telematics to underwrite risk has the potential to blur the lines around insurer knowledge, whilst the increased robotisation of distribution channels allows the insured to take a passive role in the disclosure process. This could undermine an insurer’s ability to defend claims for breach of the duty of fair presentation.
- The use of AI and machine learning to analyse risk gives rise to concerns on data privacy, cyber security, fairness and discrimination. In September 2016, and following its Call for Inputs in the use of Big Data in the general insurance sector, the FCA raised concerns that the micro-analysis of risk through the use of technology could lead to a new group of “uninsurables”. The FCA also warned that insurers could leverage the data to charge higher premiums unreflective of the risk. The FCA committed to intervene if either scenario became a reality.
- There are a number of features of blockchain and smart contracts which are at odds with insurance law and regulation. In particular, the immutable nature of DLT gives rise to obvious data protection issues and conflicts directly with the “right to be forgotten” in the General Data Protection Regulation (“**GDPR**”). The automation of claims through a smart contract may also make it difficult for an insurer to demonstrate to the FOS or the courts that its refusal to pay a claim was appropriate.

These legal and regulatory considerations have led to increased scrutiny by the FCA into the use of technology in the insurance value chain. Whilst this could give rise to the potential for increased regulatory intervention, the FCA has instead adopted an open-house approach and its sandbox has provided a safe space for a number of InsurTechs to test out their products in a supportive regulatory setting. Nevertheless, we can expect the FCA to continue to keep a close eye on technological developments in the insurance sector as well as further guidance from industry bodies, such as the Association of British Insurers (“**ABI**”) and the British Insurance Brokers Association (“**BIBA**”), and from the English courts as they struggle to apply the existing statutory framework to non-traditional insurance products.

Regulatory bodies

In the UK, there is no single regulatory framework which governs FinTech. Instead, consideration needs to be given to the way in which FinTech is adopted in the facilitation and delivery of financial services.

FinTech firms which carry on certain regulated activities¹ (including, for example, consumer credit-related activities, banking, advising on investments, insurance distribution, etc.) will fall within the regulatory perimeter, unless an exemption applies, and will need to be authorised and regulated by one or more of the following bodies:

- the FCA – the FCA’s key focus is on the risks posed by the conduct of financial services firms, and the individuals which work for them, to its three statutory objectives: protecting consumers; ensuring market integrity; and promoting effective competition. Any firm which carries on regulated activities by way of business in the UK will need to be authorised and regulated by the FCA. At present, the FCA regulates the conduct of approximately 58,000 businesses; and
- the Bank of England (“**BoE**”) – the BoE, through the Prudential Regulation Authority (the “**PRA**”), aims to ensure the financial soundness of firms and seeks to remove or reduce systemic risks that may threaten market stability. While the FCA focuses on conduct risk, the PRA focuses on the prudential soundness of firms. Only those firms which pose a systemic risk will need to be authorised by the PRA which, at present, regulates approximately 1,500 banks, building societies, credit unions, insurers and major investment firms.

In the UK, it is a criminal offence to carry on regulated activities by way of business (unless an exemption applies) without first obtaining authorisation from the FCA and, if applicable, the PRA.

Policy surrounding financial services regulation is driven by HM Treasury (“**HMT**”) and, although they work independently of it, each of the BoE, FCA and PRA work closely with HMT to maintain and develop the UK’s financial services legislative and regulatory framework.

Key regulations and regulatory approaches

There is no single regulatory framework which governs FinTech firms. Instead, the extent to which FinTech firms are regulated will depend on the nature of the activities which they conduct, and the nature, scale and size of their business. As a starting point, therefore, FinTech firms should consider whether, and to what extent, they fall within the UK’s regulatory perimeter and, if necessary, apply for the relevant authorisation from the UK regulator(s).

The Financial Services and Markets Act 2000 (“**the Act**”) establishes the FCA and the PRA as the statutory regulators of UK financial services businesses and provides them both with each of their statutory powers, including their general power to make rules under the Act. These rules are extensive and are largely embodied within the FCA’s Handbook of Rules and Guidance and the PRA’s Rulebook. FinTechs which require authorisation will need to understand the rules which are most applicable to their businesses and comply with them accordingly. A failure to do so could result in enforcement action being taken by the FCA and/or the PRA and penalties include significant fines and, in the cases involving individuals, potential prohibitions from working in the industry altogether.

While, generally, the FCA’s and PRA’s rules are technology neutral, the rise in the number of FinTech firms in recent years has led to two important regulatory developments: the first has been in the form of greater clarity on the regulatory approach to cryptoassets, which has been one of the biggest applications of technology in the financial services space over the last few years; and the second is in the form of forthcoming changes in the UK’s anti-money laundering regime, both of which we consider further below.

In general terms though, the UK financial regulators and policy makers are very receptive to FinTech. HMT has recognised that the FinTech sector has the capacity to deliver huge benefits across society, driving greater competition by harnessing the latest technologies to deliver faster and better financial services. In March 2018, HMT launched its Fintech Sector Strategy in an attempt to secure the future of UK Fintech and make the UK attractive to FinTech businesses.

This governmental approach has influenced the approach of the FCA and PRA. In particular, the FCA is generally regarded as one of the leading regulators in this area through the creation of “Project Innovate” in October 2014, with a dedicated team working across all of its three core innovation initiatives:

- a “Regulatory Sandbox” which is open to authorised firms, unauthorised firms that require authorisation, and technology businesses allowing firms the ability to test their business models, products and services in a controlled environment, closely overseen by the FCA;
- the “Advice Unit” which provides regulatory feedback to firms developing automated models to deliver lower-cost advice and guidance to consumers; and
- the “Innovation Hub” which provides a dedicated contact for innovator businesses that are considering applying for authorisation or a variation of permission, need support when doing so, or do not need to be authorised but could benefit from support.

While the FCA, PRA and HMT are embracing FinTech to further competition in the interest of UK consumers and the UK economy as a whole, they are also taking certain precautionary steps as outlined below.

Regulatory approach to cryptoassets

In March 2018, the Chancellor of the Exchequer launched the Cryptoassets Taskforce (“**the Taskforce**”) in response to the significant attention being given to DLT and the rise in the number of cryptoassets. The Taskforce comprised HMT, the FCA and the BoE and, together, they produced a final report in which it concluded that DLT has the potential to deliver significant benefits in financial services and other sectors. However, they warned that the regulators would take action to mitigate the risks that cryptoassets can pose to consumers and market integrity: to prevent the use of cryptoassets being used for illicit activity; to guard against the threats to financial stability that could emerge in the future; and to encourage responsible development of legitimate DLT and cryptoasset-related activity in the UK.

Clarity on the regulatory perimeter

In January 2019, the FCA published a consultation paper² that sets out guidance on how cryptoassets can be subject to its regulation (“**the Guidance**”). The Guidance is relevant to any firm issuing, creating, buying, selling, holding or storing cryptoassets, firms marketing cryptoasset products and services, as well as their advisers.

The Guidance will, once final, clarify where different categories of cryptoasset tokens fall in relation to the FCA’s regulatory perimeter – i.e., the boundary that separates regulated and unregulated financial services activities. Activities that fall within the regulatory perimeter are regulated and require authorisation from the FCA – and in limited circumstances the PRA – before they can be carried out.

The FCA has categorised cryptoassets into three types of tokens and has provided guidance on whether these tokens are regulated or unregulated. In categorising cryptoassets as below, the FCA has made clear that the categories of token are not mutually exclusive, nor are they exhaustive of the types of cryptoassets that can exist. Whether a cryptoasset falls within the

regulatory perimeter should always be considered on a case-by-case basis, with regard to a number of different factors.

Security tokens

Security tokens include specific characteristics that bring them within the definition of a “specified investment”,³ such as a share or a debt instrument, which means they fall within the regulatory perimeter. They include tokens that grant holders some, or all, of the rights conferred on shareholders or debt-holders, as well as those tokens that give rights to other tokens that are themselves specified investments. The FCA considers a security to refer broadly to an instrument that indicates an ownership position in an entity, a creditor relationship with an entity, or other rights to ownership or profit. Security tokens are securities because they grant certain rights associated with traditional securities.

FinTech firms which carry on a regulated activity involving security tokens will need to make sure that they are appropriately authorised or exempt. Issuers of such tokens may themselves not need to be authorised; however, certain requirements related to the issuance of the tokens may still apply – for example, prospectus and transparency requirements.

Factors to consider when determining if a token is a security token

Given the complexity of many tokens, the FCA has recognised that it is not always easy to determine whether a token is a specified investment. The FCA has, therefore, set out a non-exhaustive list of factors that it considers are indicative of a security to assist firms in determining whether or not they are undertaking regulated activities:

- the contractual rights and obligations the token-holder has by virtue of holding or owning that cryptoasset;
- any contractual entitlement to profit-share (e.g. dividends), revenues, or other payment or benefit of any kind;
- any contractual entitlement to ownership in, or control of, the token issuer or other relevant person (e.g. voting rights);
- the language used in relevant documentation (e.g. white papers). However, the FCA has made clear that if a white paper declares a token to be a utility token, but the characteristics of the token indicate it is a specified investment, the FCA would treat it as a security token;
- whether the token is transferable and tradeable on cryptoasset exchanges or any other type of exchange or market;
- whether there is a flow of payment from the issuer or other relevant party to token holders; and
- whether any flow of payment is a contractual entitlement – the FCA has made clear that it would consider this to be a strong indication that a token is a security.

Exchange tokens

Exchange tokens are not issued or backed by any central authority and are intended to be designed to be used as a means of exchange. These tokens can enable the buying as well as selling of goods and services without the need for traditional intermediaries, such as central or commercial banks (e.g., on a peer-to-peer basis).

Exchange tokens are used in a way similar to traditional fiat currency. However, while exchange tokens can be used as a means of exchange, they are not currently recognised as legal tender in the United Kingdom, and are therefore not considered to be “currency” or “money” within the UK regulatory framework. Due to the fact that they tend to be

decentralised, with no central issuer obliged to honour contractual rights, the FCA's view is that they do not typically grant the holder any of the rights associated with "specified investments".

As such, the FCA has confirmed that exchange tokens generally fall outside of the regulatory perimeter. Therefore, transferring, buying and selling these types of token, including the commercial operation of cryptoasset exchanges for exchange tokens, are activities not currently regulated by the FCA. However, they may be caught by the UK's anti-money laundering regime in the future (see further below).

Utility tokens

Utility tokens provide holders with access to a current or prospective product or service but do not grant holders rights that are the same as those granted by specified investments. They may have similarities with rewards-based crowdfunding where participants contribute funds to a project in exchange for a reward; for example, access to products or services at a discount.

The FCA has stated that, much like exchange tokens, utility tokens can usually be traded on the secondary markets and can be used for speculative investment purposes. However, this does not mean these tokens constitute specified investments.

Although utility tokens do not typically exhibit features of specified investments, they could still require FCA authorisation if they constitute "e-money" or are used to facilitate regulated payment services.

Electronic money and payment services

E-money issuance is an FCA-regulated activity and, depending on how they are structured, cryptoassets can constitute e-money. E-money is electronically stored monetary value as represented by a claim on the electronic money issuer, which is:

- issued on receipt of funds for the purpose of making payment transactions;
- accepted by a person other than the electronic money issuer; and
- not excluded by the Electronic Money Regulations.

Due to the fact that they are not usually centrally issued on the receipt of funds, nor do they represent a claim against an issuer, exchange tokens like Bitcoin and Ether are unlikely to represent e-money. However, the FCA has pointed out that any category of cryptoasset has the potential to be e-money, depending on its structure and whether it meets the definition of e-money as outlined above. E-money must enable users to make payment transactions with third parties, so must be accepted by more parties than just the issuer.

Key considerations for FinTech firms

Firms which engage in activity by way of business in the UK that relates to a security token or to a token that constitutes e-money or is involved in payment services, should consider whether those activities require authorisation.

If a token is a transferable security and will either be offered to the public in the UK or admitted to trading on a regulated market, an issuer will need to publish a prospectus in accordance with the UK's Prospectus Regime unless an exemption applies.

If activities fall within the FCA's regulatory perimeter, FinTech firms should consider, in particular:

- the application of financial promotion rules, including ensuring communications are marketed in a way that is clear, fair and not misleading;

- the application of the Prospectus Directive;
- the application of relevant financial crime controls; and
- operational resilience and cyber security issues – cryptoassets are now regarded as high-value targets for theft, and service providers (e.g. custodians/wallet providers) are increasingly being targeted by cybercriminals to obtain the private keys that enable consumers to access and transfer their cryptoassets.

The UK's anti-money laundering regime

The UK's anti-money laundering (“**AML**”) regime relating to financial services is largely embodied within the Proceeds of Crime Act 2002 (“**POCA**”) and the Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 (“**the MLRs**”). The various offences are found in POCA and criminalise both the process of overt money laundering as well as the failure of otherwise legitimate businesses to report suspicions of money laundering.

The MLRs generally support the criminal money-laundering provisions in POCA. They place a general obligation on certain firms, including financial services firms, to establish and maintain appropriate and proportionate risk-based policies and procedures to prevent and detect situations where their systems may be at risk of being used in connection with money laundering. A failure to comply with the MLRs may constitute a criminal offence.

At present, cryptoassets are not generally subject to the UK AML regime. However, the Fifth Anti-Money Laundering Directive of the European Parliament and of the Council (Directive (EU) 2018/843)⁴ (“**AMLD5**”), which entered into force on 9 July 2018, extends European AML regimes to virtual currencies. Member States will have until 10 January 2020 to implement the new rules into their national legislation.

AMLD5 will capture providers engaged in exchange services between virtual currencies and fiat currencies, as well as custodian wallet providers. However, the Taskforce, in its final report, made clear that: “*the government intends to broaden the UK's approach to go beyond the [AMLD5] requirements, and will consult on including:*

1. *exchange services between different cryptoassets, to prevent anonymous ‘layering’ of funds to mask their origin;*
2. *platforms that facilitate peer-to-peer exchange of cryptoassets, which could enable anonymous transfers of funds between individuals;*
3. *cryptoasset ATMs, which could be used anonymously to purchase cryptoassets; and*
4. *non-custodian wallet providers that function similarly to custodian wallet providers, which may otherwise facilitate the anonymous storage and transfer of cryptoassets.”*

Cryptoassets are often associated with illicit activities due to the fact that digital currencies are pseudonymous, decentralised and encrypted, making it virtually impossible to track each of the transactions made, and the individual behind them. As such, the UK regulators, who consider financial crime to be a high priority risk area, are taking a more robust approach in the fight against financial crime and will be consulting on new rules in this area later in 2019.

Restrictions

Although the UK regulatory authorities have encouraged the development of FinTech, they have also raised concerns about the risks posed by FinTech in some areas. The FCA identified a number of risks relating to cryptoassets in its 2019 Consultation Paper:

Harm to consumers – cryptoassets such as token-based investments are typically highly speculative and volatile. Consumers may experience unexpected or large losses. Leveraged derivatives, like Contracts for Differences (“CFDs”) and futures, referencing cryptoassets carry a high risk of loss. The white papers documents that typically accompany ICOs are not standardised and may omit significant information such as the risks posed by the investments.

The FCA has issued various consumer warnings. For example, in June 2018 the FCA published a warning to consumers about cryptocurrency investment scams. The FCA (also in June 2018) wrote to the CEOs of banks warning of the risk of abuse of cryptoassets. Banks were warned to take reasonable and proportionate measures to lessen the risk that they might facilitate financial crimes that are enabled by cryptoassets. We understand this has resulted in some cryptoasset firms finding it harder to obtain bank accounts, with more scrutiny involved.

Financial crime – Poor cyber security can result in hacking of custodians and wallet providers to obtain private keys which enable consumers to access and transfer their cryptoassets. Also, cryptoassets tend to offer potential anonymity and sometimes lack transparency. This makes them attractive for money laundering and harder to detect. Europol estimates that £3–4 billion is laundered using cryptoassets each year in Europe.

Market integrity – Market volatility (see for example the volatility of Bitcoin) and the lack of transparency increases the potential risk of market manipulation and insider dealing on exchanges and trading platforms. For example, “pump and dump” schemes have become increasingly prevalent in cryptocurrency markets. An analysis by the *Wall Street Journal* identified 175 pump and dump schemes involving 121 different digital coins between January–July 2018.

Cross-border business

Cross-border FinTech investment increased more than three times in 2018, with well over 2,000 transactions taking place with an aggregate value of over £40 billion between them. In 2019, we have seen the following trends:

- The UK remained the leading investment destination in Europe, but moderate growth has continued throughout the continent.
- The USA has continued to drive investment in North and South America, although Canada and Brazil have also seen transactions reach record levels.
- The most significant growth has been seen in Asia, especially in India, China and Singapore, which have been leading destinations for innovation, with skilled personnel driven by greater governmental investment in research & development and global expansion.

Going forward, we expect to see the following themes:

- The size of cross-border FinTech transactions will increase as investors look more at FinTech firms that are more established in the market in order to minimise risk.
- Following the growth of USA and European FinTech-driven challenger banks over the past few years, they will look to expand their reach to foreign countries and increase the types of services they offer.
- Asia will continue to see huge growth in transactions and investments particularly because of innovative home-grown businesses, and also because mainstream financial

services companies in the USA and Europe will seek to experiment with new FinTech services in the region.

- The rise of financial services hubs outside the traditional centres such as New York and the City of London, as decentralisation takes place driven by the Amazon generation into locations less conventionally known for their developed financial services industries.

Co-operation between regulators – the Global Financial Innovation Network

Given the increasing number of FinTech firms which were seeking to offer cross-border solutions to customers, in early 2018, the FCA proposed the creation of a global version of its regulatory sandbox. After a period of consultation with industry, the GFIN was formally launched in January 2019 by an international group of 35 financial regulators and related organisations, including the FCA, all of which are committed to supporting financial innovation in the interests of consumers.

The GFIN aims to provide a more efficient way for innovative firms to interact with regulators, helping them to navigate between countries as they look to scale their businesses. This includes a pilot for firms wishing to test innovative products, services or business models across more than one jurisdiction. Similar to the FCA's regulatory sandbox, the GFIN would essentially offer firms successfully making it onto the programme, a safe environment in which to trial cross-border solutions. This could potentially reduce the time and costs for FinTech firms when bringing innovative ideas to, and launching business models in, new international markets. It also aims to create a new framework for co-operation between financial services regulators on innovation-related topics, sharing different experiences and approaches.

Acknowledgments

The authors would like to thank David Brennan and Dhruv Chhatralia for their contribution to this chapter.

David is a partner in the corporate team and Co-Chair of the firm's global tech Group. His practice focuses on both equity capital markets and public and private mergers and acquisitions. He has advised both issuers and sponsors on numerous IPOs and secondary fundraisings (including placings, open offers and rights issues), particularly of AIM and dual listed companies. He has considerable experience advising on public takeovers, private acquisitions and disposals and international joint ventures in various sectors, but with a particular emphasis on tech.

Dhruv is a principal associate in the Corporate practice of Gowling WLG based in the London office. Dhruv has over 10 years' experience advising on mergers and acquisitions, private equity transactions, corporate finance transactions, joint ventures, and other areas of corporate law. He works on both domestic and cross-border transactions representing corporates, private equity houses and financial institutions. Dhruv acts for clients in a variety of sectors including technology, media and telecommunications, financial services, energy, natural resources, infrastructure and projects, automotives, life sciences, and hotels and leisure.

* * *

Endnotes

1. Regulated activities are specified by the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001.
2. FCA Guidance on Cryptoassets consultation paper (CP19/3), dated January 2019.
3. Any of the investments specified in Part III of the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (SI 2001/544).
4. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L0843>.

**Ian Mason****Tel: +44 20 7759 6685 / Email: ian.mason@gowlingwlg.com**

Ian is a Partner and Head of UK Financial Services Regulatory Team at Gowling WLG.

Ian has more than 20 years advising clients on financial regulation, and is a former Head of Department in the Enforcement Division at the UK financial services regulator, as well as having worked in-house, and advising firms and individuals in private practice. Ian has been involved in advising a number of FinTech clients on regulatory issues, including regulatory perimeter advice, anti-money laundering provisions, payment services and e-money. His clients include banks, asset managers, brokers and listed companies. Ian has significant experience in advising clients on regulatory investigations, both in enforcement and on the defence side, representing firms and individuals.

**Sushil Kuner****Tel: +44 20 7759 6542 / Email: sushil.kuner@gowlingwlg.com**

Sushil is a Senior Associate in the Financial Services Regulatory Team at Gowling WLG.

Sushil joined Gowling WLG in July 2018, having spent eight years working within the Supervision and Enforcement Divisions of the FCA. She has a wealth of regulatory experience across a broad range of contentious and non-contentious issues, offering clients a holistic approach to regulatory compliance and the ability to spot risks before they arise. She advises on all aspects of financial services regulatory law and has a particular interest in FinTech, advising a number of clients on regulatory considerations for ICOs, blockchain and cryptoassets since joining. Sushil regularly represents the firm at FinTech and blockchain events, most recently moderating and participating in a panel discussion at FinTech Connect, one of the largest annual FinTech conferences in the UK, and has written a number of FinTech-related client alerts and articles.

**Samantha Holland****Tel: +44 37 0733 0590 / Email: samantha.holland@gowlingwlg.com**

A Partner in the Insurance Team, Samantha chairs the Gowling WLG InsurTech Group which combines an understanding of technologies such as blockchain, AI and IoT with in-depth knowledge of the insurance value-chain and the regulatory framework in which InsurTechs operate. These leading technology and insurance professionals provide full-service legal support across the InsurTech landscape. Samantha innovates wherever possible working with entrepreneurial clients to bring products to market, most recently in the sports insurance, transactional insurance and financial services markets. Her 18 years as a litigator mean that she is ideally placed to analyse risk and stress-test the application of new technologies.

Gowling WLG

4 More London Riverside, London SE1 2AU, United Kingdom
Tel: +44 37 0903 1000 / Fax +44 370 904 1099 / URL: www.gowlingwlg.com

USA

Barbara Stettner, Hilary Sunghee Seo & Jonathan Flynn
Allen & Overy LLP

Approaches and developments

Evolutionary approach to regulatory innovation

The U.S. financial regulatory framework is fragmented, with oversight and regulation divided and shared among various federal and state agencies, each with a specific mission, mandate and regulatory philosophy. As described in more detail below in “Regulatory bodies”, federal and state banking regulators (including the U.S. Office of the Comptroller of the Currency (**OCC**) and the New York Department of Financial Services (**NYDFS**)), anti-money laundering authorities (e.g., the Financial Crimes Enforcement Network (**FinCEN**)), the U.S. Securities and Exchange Commission (**SEC**), the U.S. Commodity Futures Trading Commission (**CFTC**), and others are currently in the process of defining the regulatory landscape for new technologies in the United States and, indirectly, exerting significant influence over the landscape around the globe. That said, there is no definitive consensus view across agencies, and it is unlikely that such a consensus will form in the foreseeable future. Instead, fragmentation means that regulatory change will occur, but it will more likely happen incrementally through an evolution of each agency’s exercise of jurisdiction over those it regulates directly rather than through a revolutionary shift from one paradigm to another.

The adoption of new technologies in the financial markets that are collectively and commonly known as Fintech is no exception. Rather than adopt entirely new regulatory frameworks, federal and state regulators in the United States have largely sought to apply existing regulatory principles to Fintech, with varying levels of success. One particular and fundamental challenge is that many new financial technologies are built on the premise that greater decentralisation of institutions and infrastructure will lead to greater efficiency and utility in the marketplace. But the socialisation of core market functions is at odds with many traditional regulatory regimes, which rely upon a relative few, well-regulated intermediaries, such as banks, brokers, exchanges and central clearinghouses, and depository institutions to act as gatekeepers so as to ensure the integrity of the system as a whole.

Examples of regulatory evolution

Finding a way to translate long-standing (and sometimes overlapping) regulatory regimes into new, disintermediated financial technologies is the most basic and important challenge facing U.S. Fintech developers in the United States. Two specific examples in the custody space highlight the issues and challenges in achieving this goal:

(a) Custody of crypto assets that are or could be securities subject to the SEC’s jurisdiction

Brokers and investment advisers who hold client assets consisting of securities are subject to regulations regarding the custody of those assets, including that they be maintained in a good control location that provides the requisite assurance that the securities are safe and

secured. A confounding challenge for market participants and regulators has been identifying custody solutions that not only satisfy, but can be demonstrated to satisfy, this standard where the thing that is being custodied is digital in nature.

Senior SEC officials, including Chairman Jay Clayton, have expressed concerns about the custody of crypto-assets that are or may be securities at broker-dealers, particularly for retail investors, and have indicated a preference to push custody of those assets into a non-broker-dealer custodian, such as a bank.

This solution, however, would trigger regulatory complications under the current legal structure. Without an exception or exemption, providing custody of customer securities is a regulated activity that requires registration with the SEC as a broker-dealer and authorisation by the Financial Industry Regulatory Authority (**FINRA**)¹ to conduct business as a carrying broker. A bank providing custodial services and deposit-taking or fiduciary services generally would enjoy a statutory exception from broker-dealer registration with respect to crypto-assets that constitute securities, but this exception would appear not to be available where there is no broker-dealer in the chain performing the role of carrying broker-dealer with respect to the crypto-assets, due to a statutory carve-out to the exception from registration. It is unclear whether these issues have been fully thought through by the regulators. Noting the SEC's lag in directing the industry, SEC Commissioner Hester Peirce recently pointed out that the SEC's silence could stifle innovation and ultimately prove fatal to certain cryptocurrency custody efforts.

(b) Custody of virtual currencies associated with futures contracts overseen by the CFTC

Similarly, the CFTC has expressed concerns regarding custody of Bitcoin by entities other than state- or federally regulated trust companies as a result of physical settlement of Bitcoin futures contracts.² Thus, while the CFTC has not moved to block listings of *cash* settled Bitcoin futures,³ efforts by exchanges to list *physically* settled Bitcoin futures have stalled as exchanges seek to resolve regulatory objections.⁴ Although the CFTC has not commented publicly on any proposed listing, CFTC Chairman J. Christopher Giancarlo has indicated that the CFTC feels bound by its statute and existing regulations to ensure that exchange customers have the option to custody assets (including physically delivered Bitcoin) with a bank or trust company rather than the exchange's clearinghouse if they so choose.⁵ For this reason, Bakkt, a nascent Bitcoin futures exchange developed in partnership with the Intercontinental Exchange (**ICE**), is reportedly seeking to become a state-chartered trust company to satisfy CFTC objections to its efforts to list one-day, physically settled Bitcoin futures cleared through ICE.⁶

Together, these examples illustrate a broader trend. Although regulators are generally open to the adoption of new financial technologies, they remain wary of taking firm positions unless the risks of potential failures or gaps posed by new technology that could cause market disruption, compliance lapses, or customer harm have been fully contained or shifted to another regulator. Such concern has, at times, resulted in regulatory paralysis.

Fintech offering in the United States

Although some applications are more developed and mature than others, Fintech is making inroads into virtually every aspect of the financial marketplace, often raising significant regulatory issues and challenges in the process.

Rise of the machines

Automatic trading systems in futures markets

Mirroring the trend in the cash equity markets, automated trading systems (**ATS**) have come

to dominate futures markets over the past decade, particularly with respect to financial asset classes such as equity and interest rate futures, which now see as much as 90% of all orders executed by an ATS.⁷ The rise of automated trading has created its own set of regulatory concerns and challenges. Chief among these are instances of flash crashes and market manipulation resulting from malfunctioning trading algorithms or disruptive trading practices, including spoofing.⁸

In reaction to concerns that ATS could pose threats to market integrity, the CFTC has considered regulating automated trading, going so far as to propose a rule that would have required automated traders, clearing brokers, and exchanges to implement automated trading risk controls, imposed registration obligations on certain proprietary traders engaged in algorithmic trading on an ATS, and, notably, would have authorised CFTC staff to obtain proprietary algorithm source code upon request without a subpoena or other legal process, among other things.⁹ In November 2016, the CFTC proposed amendments that moderated its original proposal, suggesting the establishment of a trading volume threshold for subjecting industry participants to the rule's most onerous provisions, and requiring CFTC staff to obtain Commission approval for a subpoena or special call in order to access algorithm source code.¹⁰ Thus far, the CFTC has not acted to finalise the rule, however, opting instead to collect data on large trading positions on a daily basis and pursue enforcement actions for flash crashes and spoofing incidents.

Robo-advisers

Automation has also assumed a prominent role among investment advisory products, where automated investment advisory platforms (often called robo-advisers) are gaining significant market share.¹¹ Assets under automated management are expected to reach \$5 trillion to \$7 trillion by 2025.¹² Recognising this trend, the SEC Office of Compliance Inspections and Examinations (**OCIE**) 2018 examination cycle included a focus on investment advisers and broker-dealers that offer investment advice through automated or digital platforms, such as robo-advisers and other firms that interact primarily with clients online. Examinations focused on such advisers' compliance programs, including the oversight of computer algorithms that generate recommendations, marketing materials, investor data protection, and disclosure of conflicts of interest.¹³ This initiative followed on from 2017 guidance for robo-advisers from the SEC Division of Investment Management, which emphasised the need for clarity and thoroughness in:

- (a) disclosures regarding the assumptions underlying any algorithms used, any limitations of such algorithms, and the degree of human involvement in the advisory services provided (among other information); and
- (b) questionnaires used to elicit a client's financial objectives in order to generate investment advice.¹⁴

Electronic and virtual currency and payments

Many Fintech developments implicate, directly or indirectly, virtual or crypto currencies and the integration of blockchain technology into modern payment systems. The most basic elements of these emerging markets are the exchanges on which virtual currencies are traded and the intermediaries that permit virtual currencies to be exchanged for fiat currencies. Exchanges for virtual currency derivatives that would permit hedging and speculation on a leveraged basis are also being established, but each new category of activity presents a combination of regulatory issues, both new and old.

(a) Spot markets and actual delivery

Many platforms offering spot (i.e., cash-market) virtual currency trading also wish to provide

the ability to trade on a leveraged or margined basis, meaning that a trading counterparty (or a person acting in concert with the counterparty) would finance a portion of a customer's virtual currency position. Spot trading of virtual currencies is currently subject to minimal regulation.¹⁵ Section 2(c)(2)(D) of the Commodity Exchange Act (CEA) limits leveraged spot trading in commodities to be offered only on a designated contract market (DCM) – i.e., a futures exchange registered with the CFTC – unless such leverage is offered and provided only to certain types of sophisticated non-retail investors (“eligible contract participants” (ECP)) or there is actual delivery of the commodity within 28 days following execution of the trade.¹⁶ Because virtual currencies have been identified as commodities under the CEA¹⁷ and the virtual currency trading platforms in question are not DCMs, Section 2(c)(2)(D) precludes the platforms from offering leveraged spot trading to retail participants unless they satisfy the actual delivery exception.

The concept of actual delivery has proven difficult to define in practical terms. This is particularly true with respect to delivery of Bitcoin and similar virtual currencies, which are held in digital wallets controlled by cryptographic private keys. In a June 2016 enforcement action against BFXNA Inc. (**Bitfinex**), the CFTC took the position that settling Bitcoin to a digital wallet is insufficient for actual delivery if the exchange or the seller controls all private keys associated with the wallet.¹⁸ Following *Bitfinex*, the CFTC responded to requests for greater clarity as to its views on actual delivery in the context of virtual currencies by issuing a proposed interpretation on the subject.¹⁹ In this proposal, the CFTC took the position that actual delivery is not accomplished if the counterparty seller or anyone acting in concert with the seller retains an interest in or control over any portion of the commodity after 28 days have elapsed following the transaction date.²⁰ Thus, under the proposed guidance, a seller that retains a lien on any portion of the commodity at the expiration of 28 days following the transaction cannot be said to have made actual delivery, even if the buyer receives title to the commodity and is free to lend or resell it subject to the lien.²¹

In the interim, while the CFTC considers whether and how to revise its proposed guidance on the meaning of actual delivery, the U.S. Court of Appeals for the Ninth Circuit has heard oral arguments in the appeal of a potentially significant case concerning actual delivery, albeit outside the context of virtual currencies.²² In *CFTC v. Monex*, the CFTC is appealing a loss in a lower court,²³ arguing that Monex's practice of transferring precious metals bought or sold on margin to a third-party depository and passing title to the buyer was insufficient for actual delivery because customers did not have contractual rights to the metal until they paid for it in full, even if such repayment occurred more than 28 days after execution of the transaction.²⁴ Monex responded that this view is inconsistent with the CFTC's 2013 interpretation of the term actual delivery in the context of retail commodity transactions generally, as the 2013 interpretation concluded that actual delivery would occur if a seller physically delivered the commodity to an unaffiliated depository and transferred title to the commodity to the buyer.²⁵ The Ninth Circuit has not yet issued a decision in the case.

(b) Case study: jurisdictional limits to being “located in the United States”

Some trading platforms seeking to offer new leveraged spot or derivatives products to retail customers have attempted to avoid direct U.S. regulation by establishing an exchange outside the territorial United States and restricting the ability of individuals located in the United States to access the system. Section 4(a) of the CEA makes it unlawful to execute trades in futures other than on a DCM unless such futures contracts are made on or subject to the rules of a board of trade, exchange, or market that is located outside the United States.²⁶ This prohibition on off-exchange trading applies equally to leveraged or margined spot

trading in any commodity, including virtual currencies,²⁷ unless there is actual delivery of the commodity within 28 days of execution of the trade, as discussed above.²⁸

The CFTC has declined to adopt a bright-line test for determining when a platform is located outside the United States and thus excluded from the prohibition on off-exchange futures trading under CEA Section 4(a).²⁹ Instead, the CFTC considers the totality of factors presented by the particular platform.³⁰ In adopting this position in a 2006 policy statement (**2006 Policy Statement**), the CFTC notably emphasised the need to accommodate rapid changes in technology as well as global business structures and relationships, reasoning that determining an exchange's location on the basis of one specific factor, such as the location of technology used to operate the exchange, could inhibit structural and technological innovation.³¹ The CFTC also acknowledged commenters' views that it would make little sense to use the location of an exchange's technological infrastructure, including its matching functions, as a proxy for the location of the exchange itself, as such functionalities are likely to change locations over time and lend themselves to outsourcing to technology vendors.³² How this guidance will be applied in practice will ultimately be determined through a combination of enforcement actions and informal staff guidance in the form of no-action letters and interpretive statements.

(c) Non-traditional payment systems

Fintech is fostering other types of non-traditional payment systems that promise to be more efficient or useful than traditional methods. Prepaid and non-prepaid debit cards, credit cards, automated clearinghouse (ACH) system credit and debit transfers, and checks compose a core set of non-cash payment types commonly used today by consumers and businesses in the United States. These payment types are used both in traditional ways, such as in-person purchases and payroll deposits, and in relatively new ways, such as mobile and e-commerce payments.³³ Since 2000, consumers and businesses in the United States have substantially changed their payment choices, with check payments primarily being replaced with card payments and electronic transfers via the ACH system. Fifty-one per cent of mobile banking users deposited a cheque using their mobile phone in 2014, up from 38% in 2013, and 39% of those users also reported making a payment with a mobile barcode scanner.³⁴ As already noted, virtual currencies including Bitcoin and others have also begun to shape the payments landscape in the U.S.³⁵

While such transactions are susceptible of a variety of different characterisations, when conducted by an organisation other than a U.S. bank, most states require licensing under a regime focused on the protection of local consumers and ensuring that money-laundering risks are minimised. Such activities also require registration as a "Money Services Business" with FinCEN, as well as the establishment of a comprehensive anti-money laundering programme subject to compliance with FinCEN's regulations.

Regtech developments

New technology has made financial market surveillance more pervasive and more effective. The adoption of powerful new surveillance tools by regulators and self-regulatory organisations has effectively raised the bar for all participants in the financial markets.

The SEC and the CFTC (and the exchanges they regulate) have developed sophisticated systems to monitor their markets and automatically identify trading behaviour that is abnormal and suggestive of prohibited activity. For example, the CFTC recently realigned its Market Surveillance Branch to be housed within its Division of Enforcement. This reorganisation was intended to allow the CFTC to use its sophisticated market surveillance technology to analyse trade data and respond to outlying events that warrant further enforcement inquiry.

FINRA report regarding technology-based innovations for regulatory compliance in the securities industry

Exchanges and other self-regulatory organisations are following a similar course. For example, in September 2018, FINRA published a report on technology-based innovations for regulatory compliance (**Regtech**) in the securities industry.³⁶ The report summarised how Regtech tools are being applied in the following five areas:

- surveillance and monitoring;
- customer identification and anti-money laundering compliance;
- regulatory intelligence;
- reporting and risk management; and
- investor risk assessment.

The FINRA report noted that while Regtech tools may facilitate the ability of firms to strengthen their compliance programs, they may also raise new challenges and regulatory implications for firms to consider. For example, Regtech applications may use highly complex and sophisticated AI algorithms, which are designed to learn and evolve based on data patterns. However, compliance and business professionals may not have the technical skills to understand in detail how these algorithms function, posing challenges to firms' governance, supervision, risk management, and training infrastructure and practices.

Monitoring employees of regulated firms

Regulated firms are also increasingly using technology to monitor employees' business communications (e.g., emails, instant messages, and phone conversations). The SEC's OCIE has also recognised this trend and responded by issuing examination observations in December 2018³⁷ on the use of electronic messaging. These observations identified examples of practices that the OCIE staff believes may assist advisers in meeting their recordkeeping obligations under the Investment Advisers Act of 1940, including:

- (a) Contracting with software vendors to monitor employee social media posts, emails, or websites, archiving such business communications to ensure compliance with record retention rules and identifying any changes to content, and comparing messages to a lexicon of key words and phrases.
- (b) Regularly reviewing popular social media sites to determine whether employees are using the media in violation of the adviser's policies.
- (c) Running regular Internet searches or setting up automated alerts to notify the adviser when an employee's name or the adviser's name appears on a website, in order to potentially identify unauthorised advisory business being conducted online.
- (d) Establishing a confidential means by which employees can report concerns about a colleague's electronic messaging, website, or use of social media for business communications.

All U.S. financial regulators are closely focused on implementation of reasonable supervisory systems and procedures for reviewing electronic communications. FINRA, for example, has urged member firms to consider using a combination of lexicon-based and random reviews of electronic correspondence³⁸ and has fined member firms as much as \$2 million for failing to maintain reasonably designed supervisory systems and procedures for reviewing electronic communications.

Digital legal identity

Separately, the U.S. Department of the Treasury is advocating an initiative that would

facilitate the adoption of trustworthy digital legal identity (**DLI**) products and services in the financial services sector. By employing electronic means to unambiguously assert and authenticate a real person's unique legal identity, DLI products and services would improve the trustworthiness, security, privacy, and convenience of identifying individuals and entities in the Fintech space, thereby strengthening the processes critical to the movement of funds, goods, and data as the global economy moves deeper into the digital age.³⁹ Trustworthy digital identity systems could be a critical compliance tool to aid Treasury's FinCEN in its enforcement of anti-money laundering (**AML**) and sanctions regulations, as they would significantly improve customer identification and verification for onboarding and authorising account access, general risk management, and the anti-fraud efforts of Fintech companies.⁴⁰

Use of Regtech in the AML space

In addition, on May 24, 2019, FinCEN announced that it would begin holding monthly "Innovation Hours" designed to offer financial institutions as well as Fintech and Regtech companies the opportunity to present to FinCEN their innovative products, services, and approaches designed to enhance AML efforts.⁴¹ The programme is intended to improve public- and private-sector understanding of the opportunities and challenges associated with AML innovation.

Regulatory bodies

The U.S. financial regulatory landscape is highly fragmented and includes overlapping jurisdiction, with oversight of various parts of the financial system divided among a variety of federal and state regulators.

Federal banking regulators

Federal regulation of banking institutions is divided among several agencies, chief among these being the Federal Reserve Board (**FRB**), the Federal Deposit Insurance Corporation (**FDIC**), and the OCC. Each agency serves as the primary federal prudential regulator for certain types of banking entities. One or more other agencies may serve in a secondary regulatory role with respect to that institution.

The key entities under the FRB's jurisdiction include bank holding companies (i.e., parent companies of insured depository institutions) and their nonbank subsidiaries, foreign banking organisations operating in the United States (including through a state-licensed branch or agency), and state-chartered banks that are members of the Federal Reserve System (which provides payment and other services to member institutions). The FDIC is the primary regulator for state-chartered banks that are FDIC-insured but are not members of the Federal Reserve System. The FDIC also administers the federal deposit insurance fund and serves as the receiver of failed depository institutions. The OCC primarily regulates federally chartered banks (called **national banks**) and federally licensed branches of foreign banks.

SEC and FINRA

The SEC holds primary responsibility for enforcing U.S. federal securities laws and regulating the U.S. securities industry. Its primary mission is to protect investors, promote fairness in the securities markets, and share information about companies and investment professionals to help investors make informed investment decisions regarding securities transactions. The SEC regulates entities that serve as the infrastructure for securities markets, including exchanges, clearing agencies, transfer agents, central securities depositories, as well as regulated intermediaries of the securities industry, including broker-dealers and investment advisers.

The Exchange Act delegates certain regulatory authority over securities broker-dealers to FINRA as a self-regulatory organisation.⁴²

CFTC and NFA

The CFTC is the primary regulator of the U.S. derivatives markets and market participants. The CFTC directly regulates entities that serve as the infrastructure for the futures, options, and swaps markets, including exchanges, clearinghouses, and swap data repositories. In conjunction with the National Futures Association (**NFA**), the CFTC also regulates derivatives market intermediaries, including futures commission merchants (**FCM**), introducing brokers (**IB**), swap dealers, retail foreign exchange dealers, commodity pool operators, and commodity trading advisers.

FinCEN/OFAC

The U.S. Department of Treasury's FinCEN is the federal government's primary AML and counter-terrorist financing agency. FinCEN is one of the federal regulators responsible for enforcing the Bank Secrecy Act (**BSA**), the United States' primary AML statute. FinCEN also issues the BSA's implementing regulations, which detail the required AML programmatic requirements for covered Fintech companies. The U.S. Department of Treasury's Office of Foreign Assets Control (**OFAC**) is the primary administrator and enforcement agency of U.S. economic sanctions. Any U.S. person or Fintech conducting business from, through, or within the United States is subject to OFAC's jurisdiction for violations of U.S. sanctions.

CFPB

The Consumer Financial Protection Bureau (**CFPB**) administers and enforces federal consumer financial laws. The CFPB has supervisory authority with respect to such laws over banks, thrifts, and credit unions with assets over \$10 billion, as well as their affiliates. The CFPB also has supervisory authority over non-bank mortgage originators and servicers, payday lenders, and private student lenders of all sizes, among other institutions.

State regulators

State laws and regulations currently provide the primary regulatory framework for many types of banks and non-bank financial services firms deploying new and innovative technologies and products. With 50 separate legal regimes to consider, this framework can be quite fragmented. Specifically, state banking departments and financial regulatory agencies oversee and have their own laws for: consumer finance companies; money services businesses (**MSBs**); debt collection businesses; and mortgage loan originators, among other types of financial entities. Regulations under these frameworks can include broadly varying firm licensing requirements, safety and soundness regulations (including permissible investments and required reserves), product limitations, interest rate limits (e.g., usury laws), examinations, and enforcement authority for violation of state and federal laws.

There are increasing efforts, however, at greater harmonisation and cooperation among state regulators. One such example is the Conference of State Bank Supervisors (**CSBS**) Fintech Industry Advisory Panel (**Advisory Panel**), which is designed to support and coordinate state regulators' increased efforts to engage with financial services companies involved in Fintech. The Advisory Panel engages with the CSBS Emerging Payments and Innovation Task Force and state regulators to identify actionable steps for improving state licensing, regulation, and non-depository supervision and for supporting innovation in financial services. In February 2019, the Advisory Panel released a series of action items to implement feedback received from the 33 companies, including creating uniform definitions and

practices, increasing transparency, and expanding the use of common technology among all state regulators.⁴³

Supra-national bodies

Although each regulatory agency carries out its mandate pursuant to its own statutory and regulatory framework, these regulatory regimes are frequently influenced by the guidance of supra-national standard-setting bodies, including the G20, the Financial Stability Board (FSB), the Basel Committee on Banking Supervision (BCBS), the International Organization of Securities Commissions (IOSCO), and the Committee on Payments and Market Infrastructure (CPMI). Many of these supra-national bodies are closely focused on Fintech and its implications for financial markets and market participants.

Recent studies published by the FSB and the BCBS, respectively, each concluded that the emergence of providers of bank-like services such as credit or payments offerings may enhance the efficiency of financial services in the longer term but could threaten the revenue bases of banks and other incumbent financial institutions, making them potentially more vulnerable to losses and reducing retained earnings as a source of internal capital. Each paper noted that the degree of disruption to incumbent banks likely depends upon the speed at which new providers enter the market.⁴⁴

Supra-national standard-setting bodies tend to be most relevant for commodities and derivatives markets because of their global nature, in contrast with the relatively parochial markets for securities and banking services. Of note, however, is the fact that the CFTC – the primary U.S. regulator for commodities and derivatives markets – does not have a seat on the FSB.

Key regulations and regulatory approaches

Federal banking regulators

The FRB was established by the Federal Reserve Act of 1913. Other key banking statutes administered by the FRB include the Bank Holding Company Act of 1956 and the International Banking Act of 1978. The FDIC was established by the Banking Act of 1933 and is governed by the Federal Deposit Insurance Act of 1950, as amended, among other legislation. The OCC was established as an independent bureau of the U.S Treasury under the National Currency Act of 1863 and administers the National Bank Act, among other laws governing national banks.

In July of 2018, the OCC announced the launch of the so-called Fintech Charter, or the agency's commencement of accepting applications for special-purpose national bank charters from non-depository Fintech companies engaged in the business of banking.⁴⁵ In practice, Fintech companies that would apply, qualify for, and receive special purpose national bank charters would be supervised in the manner of similarly situated national banks, to include capital, liquidity, and financial inclusion commitments as the OCC deems appropriate. However, the statutory authority of the OCC to issue the special charters has been challenged in litigation brought by both the Conference of State Bank Supervisors (CSBS)⁴⁶ and NYDFS.⁴⁷

SEC and FINRA

The SEC was created by the Securities Exchange Act of 1934 (**Exchange Act**). Its mission is to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation. Rather than creating a new regulatory framework for financial technologies in the securities industry, the SEC has tended to apply its existing regulatory rubric to such nascent technologies. Thus, for example, the SEC has applied the traditional test for identifying "investment contracts" under *SEC v. W. J. Howey Co.*⁴⁸ to determine whether certain types of virtual currencies are securities.⁴⁹

FINRA's mission is to promote investor protection and market integrity in the securities industry through its oversight of member broker-dealers. FINRA recently created an Office of Financial Innovation to serve as a central point of coordination for issues related to new uses of Fintech.⁵⁰ The Office will promote FINRA's engagement on Fintech issues through outreach to FINRA stakeholders, training of FINRA staff, research and publications, internal coordination across FINRA, and collaboration with other regulators.

CFTC

The CEA was first enacted in 1936 to provide a statutory framework for the regulation of trading of commodity futures in the United States. The CEA has been amended numerous times, significantly in 2010, when Title VII of the Dodd-Frank Act expanded the CFTC's regulatory authority to include over-the-counter derivative contracts (i.e., swaps). Pursuant to its statutory authority under the CEA, the CFTC has promulgated regulations that are published in title 17 of the Code of Federal Regulations.

In 2017, the CFTC created LabCFTC to serve as the focal point for the CFTC's efforts to promote responsible Fintech innovation and fair competition for the benefit of the American public.⁵¹ LabCFTC is designed to make the CFTC more accessible to Fintech innovators, and to serve as a platform to inform the Commission's understanding of new technologies. LabCFTC also functions as an information source for the Commission and the CFTC staff on new technologies that may influence policy development. According to the CFTC, the goals of LabCFTC are to promote responsible Fintech innovation to improve the quality, resiliency, and competitiveness of our markets; and to accelerate CFTC engagement with Fintech and Regtech solutions that may enable the CFTC to carry out its mission responsibilities more effectively and efficiently.

FinCEN/OFAC

FinCEN and OFAC derive their authority from a combination of statutes and regulations. *See* "Financial Crimes Enforcement Network/Office of Foreign Assets Control" above for more detail.

CFPB

Title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 created the CFPB as an independent agency within the FRB. The CFPB is charged with regulating the offering and provision of consumer financial products or services under the Federal consumer financial laws, through rulemaking as well as enforcement actions.⁵²

State regulators

In recent years, state regulators have been focused on developing greater cooperative approaches for the supervision of non-bank financial services companies. One of the primary efforts has been the development of the Nationwide Multistate Licensing System (NMLS), which is a technology platform that functions as a system of record for the licensing activities (application, renewal, and surrender) of 62 state or territorial government agencies.⁵³

Outside these cooperative efforts, some states have developed more robust frameworks than others. For example, the NYDFS has taken a particularly aggressive approach, advocating for strong state-based regulation. This posture reflects state leaders' beliefs that New York regulators have nation-leading expertise in regulating the financial services industry and protecting consumers.⁵⁴ For example, as discussed in greater detail below, NYDFS was the first state agency to release a comprehensive framework for regulating digital currency-related businesses with the implementation of BitLicenses,⁵⁵ and to date has authorised 19 companies to conduct digital currency operations.⁵⁶ New York also exemplifies the model

for state collaboration with CSBS, announcing early in 2019 that it will allow companies engaged in virtual currency business activity to use the NMLS to apply for, update, and renew their operating licences, including BitLicenses.⁵⁷

Restrictions

In addition to the general regulatory issues summarised above, several developments are worth highlighting.

Regulation of crypto assets that are securities

As discussed above, the SEC generally applies the traditional *Howey* test for identifying “investment contracts” to determine whether a particular virtual currency is a security. *Howey* asks whether participants in the offering make an “investment of money” in a “common enterprise” with a “reasonable expectation of profits” to be “derived from the entrepreneurial and managerial efforts of others”.⁵⁸ Since first adopting this approach in its investigation of the DAO “initial coin offering” (ICO),⁵⁹ the SEC has taken the view that a number of ICOs constituted offerings of securities that failed to comply with the registration requirements of Section 5 of the Securities Act of 1933.⁶⁰ In addition to facing potential liability for offers or sales of unregistered securities, a party that transmits virtual currency that is a security to purchasers on behalf of issuers or other sellers could be deemed to be acting as an unregistered broker-dealer in violation of Section 15 of the Exchange Act.⁶¹

NYDFS BitLicense requirements

In June 2015, NYDFS published its final BitLicense rules after a nearly two-year inquiry into the appropriate regulatory guidelines for virtual currency firms. Under those rules, existing virtual currency firms had until August 10, 2015 to apply for a licence. The first BitLicense was approved in September 2015. Subject to certain exceptions, anyone engaging in any of the following activities is required to obtain a BitLicense from the NYDFS: transmission of virtual currencies; storing, holding, or maintaining custody or control of virtual currency on behalf of others; buying and selling virtual currency as a customer business; performing exchange services as a customer business; or controlling, administering, or issuing a virtual currency.

Expanded regulation of money transmitters

There are currently 49 states plus the District of Columbia and Puerto Rico that impose some sort of licensing requirement in order to engage in the business of money transmission or money services. Any firm with a nationwide footprint or a purely digital presence will require a licence in, and be subject to examination by, every state in which it operates. The definition of money transmission and the corresponding licensing requirements can vary significantly by state, but generally include requirements to submit credit reports, business plans, and financial statements, as well as a requirement to maintain a surety bond to cover losses that might occur. Some states may also request information regarding policies, procedures, and internal controls. Broadly, the state regulators approach the framework with the goals of maintaining the safety and soundness of these businesses, ensuring financial integrity, protecting consumers, and preventing ownership of money transmitters for illicit purposes (e.g., money laundering or fraud).⁶²

Attempting to comply with so many varying regimes can present significant operational challenges for financial services firms. Accordingly, states have sought to harmonise examinations for money transmitters with the creation of the Money Transmitters Regulators Association (MTRA) (an association of state money transmitter regulators), which executed

a cooperative agreement in 2002 and an examination protocol in 2010 to provide for a taskforce that helps to coordinate joint money transmitter exams. As of March 2018, 48 states, Washington, D.C., Puerto Rico, Guam, and the Virgin Islands had signed the MTRA agreements. More recently, state regulators have also launched a multi-step effort to develop a 50-state licensing and supervisory system by 2020, known as Vision 2020. Goals of this plan include: establishing a Fintech Industry Advisory Panel to provide state regulators with important insight on efforts to improve state regulation; re-designing the existing NMLS platform through further automation and enhanced data and analytical tools; and developing a comprehensive state examination system to facilitate inter-state information sharing. This system is tentatively scheduled to go live in the spring or summer of 2019.⁶³

Expanded AML/BSA regulation

New financial technologies are also creating new regulatory issues that are leading regulators to apply existing authority in new ways. For example, the CFTC has historically played a relatively small role in the world of anti-money laundering and BSA enforcement, but the anonymous nature of most cryptocurrency trading has prompted the U.S. derivatives regulator to assume a more active role. This new posture was manifest in the complaint filed by the CFTC against 1Pool Ltd. (**1Pool**) and its Austrian chief executive officer on September 27, 2018. The CFTC alleged that 1Pool engaged in unlawful retail commodity transactions, failed to register as an FCM, and, notably, committed various supervisory violations under CFTC Rule 166.3 by failing to implement even basic know-your-customer procedures to prevent money laundering.⁶⁴ 1Pool was *not* a CFTC registrant, but according to the CFTC, it was nevertheless required to adopt and oversee an adequate AML programme because CFTC Rule 166.3 applies to any person who is registered *or required to be registered with the CFTC*, and 1Pool should have been registered as an FCM.⁶⁵ Moreover, because the CFTC has long taken the position that a violation of CFTC Rule 166.3 is a standalone claim that requires no underlying violation, this interpretation gives the impression that the CFTC believes that it has the authority to bring Bank Secrecy Act-related cases against any entity that is operating in a capacity that requires registration as an FCM or IB, at least through a failure to supervise a claim under CFTC Rule 166.3. This authority is in addition to the NFA's authority to audit and supervise its members in its capacity as a designated self-regulatory organisation.

The CFTC has successfully argued that cryptocurrencies are commodities and, therefore, transactions involving cryptocurrencies are subject to its jurisdiction under the Commodity Exchange Act.⁶⁶ In the complaint filed against 1Pool, the CFTC specifically noted that 1Pool failed to perform its supervisory duties diligently, as evidenced by the fact that it requires its customers to provide nothing more than a username and an email address as identifying information in order to trade on its platform.⁶⁷ In this respect, 1Pool is not unlike many cryptocurrency trading platforms that may be currently operating on an unregistered basis, even though they nominally do not solicit or accept business from the U.S. The 1Pool case highlights the importance of robust KYC procedures that are necessary to ensure banks know the true identity of their customers sufficiently to know whether they fall within the CFTC's jurisdiction and to remain in compliance with the Bank Secrecy Act.

Acknowledgments

The authors would like to thank Bill Satchell, Tracy French, Chelsea Pizzola and Catherine Thompson for their invaluable contributions to this chapter.

* * *

Endnotes

1. FINRA is a “self-regulatory organisation” established under the rules of the SEC pursuant to the Securities Exchange Act of 1934, which has the authority to establish a general supervisory framework for member firms, which includes most SEC registered broker-dealers.
2. Alexander Osipovich and Gabriel T. Rubin, *Bitcoin Futures Launch Hits Regulatory Snag*, Wall St. J., Mar. 21, 2019, <https://www.wsj.com/articles/bitcoin-futures-launch-hits-regulatory-snag-11553204037>.
3. See, e.g., CME Group, *CME Bitcoin Futures Frequently Asked Questions*, Dec. 15, 2017, <https://www.cmegroup.com/education/bitcoin/cme-bitcoin-futures-frequently-asked-questions.html>.
4. See note 2, *supra*.
5. Nikhilesh De, *CFTC Chair Giancarlo Hints at What’s Holding Back Bakkt’s Bitcoin Futures*, CoinDesk, Apr. 22, 2019, <https://www.coindesk.com/cftc-giancarlo-bakkt-bitcoin-futures>.
6. ICE Futures U.S., CFTC Submission No. 19-161: Listing of Bitcoin Monthly Futures Contract (May 13, 2019), https://www.theice.com/publicdocs/regulatory_filings/19-161_Listing_Bitcoin_Monthly_Futures_Contract%20.pdf.
7. See Market Intelligence Branch, Division of Market Oversight, CFTC, *Impact of Automated Orders in Futures Markets*, Mar. 2019, <https://www.cftc.gov/sites/default/files/2019-03/automatedordersreport032719.pdf>.
8. “Spoofing” is a manipulative practice in which a trader (or an electronic trading system designed by a trader) enters relatively small orders on one side of the market to drive the prevailing price in favour of a much larger order on the other side of the market, cancelling the smaller orders before execution.
9. See CFTC, Regulation Automated Trading (Proposed Rule), 80 Fed. Reg. 78824 (Dec. 17, 2015).
10. See CFTC, Regulation Automated Trading (Supplemental Notice of Proposed Rulemaking), 81 Fed. Reg. 85334 (Nov. 25, 2016).
11. E.g., Capgemini, *Top 10 Trends in Wealth Management 2019: What You Need to Know* (Dec. 2018), https://www.capgemini.com/wp-content/uploads/2018/11/Wealth_Management_Trends_20191.pdf.
12. Deloitte, *Hands Off, Guard Up: Robo-Advising Platforms Carry New Risks* (2017), <https://www2.deloitte.com/us/en/pages/risk/articles/robo-adviser-platform-risks-asset-wealth-management-firms.html>.
13. OCIE, SEC, *National Exam Program Examination Priorities* (2018), <https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2018.pdf>.
14. Division of Investment Management, SEC, *Guidance Update No. 2017-02: Robo-Advisers* (Feb. 2017), <https://www.sec.gov/investment/im-guidance-2017-02.pdf>.
15. Spot cryptocurrency exchanges are generally required to obtain money transmitter licences from the states in which they do business and to register with FinCEN. As discussed below, several states, including New York, have implemented licensing and regulatory regimes specifically for virtual currency businesses.
16. Section 2(c)(2)(D) of the CEA, 7 USC 2(c)(2)(D). The requirement that leveraged spot trading absent actual delivery be regulated as trading in futures does not apply where both

- parties to the trade fall within the statutory definition of an ECP (which generally includes, among other things, individuals and entities with assets exceeding \$10 million). However, even if both counterparties are ECPs, the provision of leverage may give rise to regulation generally under the CEA, e.g., if the transaction falls within the definition of a swap.
17. *E.g.*, *CFTC v. McDonnell*, 287 F. Supp. 3d 213, 228 (E.D.N.Y. 2018) (holding that the CFTC may regulate virtual currencies as commodities); *CFTC v. My Big Coin Pay, Inc.*, 334 F.Supp.3d 492, 496-98 (D. Mass 2018) (same).
 18. *In re BFXNA Inc. d/b/a BITFINEX*, CFTC Docket No. 16-19 (June 2, 2016).
 19. CFTC, Retail Commodity Transactions Involving Virtual Currency (Proposed Interpretation), 82 Fed. Reg. 60335 (Dec. 20, 2017).
 20. *Id.* at 60339-40.
 21. *Id.*
 22. *CFTC v. Monex Credit Co.*, No. 18-55815 (9th Cir. Mar. 13, 2019), https://www.ca9.uscourts.gov/media/view_video.php?pk_vid=0000015372.
 23. *CFTC v. Monex Credit Co.*, 311 F. Supp. 3d 1173, 1183 (C.D. Cal. 2018).
 24. *See, e.g.*, Amended Motion of the CFTC for Expedited Review, *CFTC v. Monex*, No. 18-55815 (9th Cir. June 21, 2018).
 25. Defendants-Appellees' Answering Brief, *CFTC v. Monex*, No. 18-55815 (9th Cir. Oct. 15, 2018).
 26. Section 4(a) of the CEA, 7 USC 6(a).
 27. *See, e.g.*, *CFTC v. McDonnell*, 287 F. Supp. 3d 213, 228 (E.D.N.Y. 2018) (holding that the CFTC may regulate virtual currencies as commodities); *CFTC v. My Big Coin Pay, Inc.*, 334 F.Supp.3d 492, 496-98 (D. Mass 2018) (same).
 28. *See* note 15, *supra*, and accompanying text.
 29. 71 Fed. Reg. 64443, 64448 (Nov. 2, 2006). In its 2011 rule providing for registration of foreign boards of trade (**FBOT**), the CFTC clarified that this 2006 policy statement remains effective, except to the extent that it endorsed the use of the no-action process rather than rulemaking to establish criteria for FBOTs seeking to provide direct access to U.S. persons. 76 Fed. Reg. 80674, 80675 n.9 (Dec. 23, 2011).
 30. 71 Fed. Reg. at 64448. While the CFTC did not identify specific factors that would be relevant to its totality of factors location analysis, it did identify certain factors that it would *not* consider probative of an exchange's location, such as the volume of trading on the exchange originating from the U.S. or the nature of the underlying contract (i.e., whether the underlying commodity is produced in or is an economically important commodity to the U.S.). *Id.* at 64449.
 31. *Id.* at 64448.
 32. *Id.* at 64448 n.49. The CFTC also noted the commenters' remarks that if the CFTC used the location of exchange technology as a jurisdictional hook, regulators in other jurisdictions may reciprocate, asserting jurisdiction over U.S. exchanges that use technology hosted in the other jurisdiction.
 33. FRB, *The Federal Reserve Payments Study 2016: Recent Developments in Consumer and Business Payment Choices*, <https://www.frb.services.org/assets/news/research/2016-payments-study.pdf>.
 34. *Id.*

35. Anton Badev & Matthew Chen, FRB, *Bitcoin: Technical Background and Data Analysis*, <https://www.federalreserve.gov/econresdata/feds/2014/files/2014104pap.pdf>.
36. FINRA, *Technology Based Innovations for Regulatory Compliance in the Securities Industry* (Sept. 2018), http://www.finra.org/sites/default/files/2018_Regtech_Report.pdf.
37. OCIE, SEC, *Observations from Investment Adviser Examinations Relating to Electronic Messaging* (Dec. 14, 2018), <https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Electronic%20Messaging.pdf>. OCIE staff specifically excluded email use on advisers' systems from its review, reasoning that firms have had decades of experience complying with regulatory requirements with respect to firm email. The staff instead focused on the increased use of social media, texting, and other types of electronic message apps, and the pervasive use of mobile and personally owned devices for business purposes.
38. *E.g.*, FINRA, Regulatory Notice 07-59: Supervision of Electronic Communications (Dec. 2007), <http://www.finra.org/sites/default/files/NoticeDocument/p037553.pdf>.
39. U.S. Department of Treasury, *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation* 41-44, 199 (2018) (**Treasury Fintech Report**), https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf.
40. *Id.*
41. FinCEN, *Press Release: FinCEN Announces Its Innovation Hours Program* (May 24, 2019), <https://www.fincen.gov/news/news-releases/fincen-announces-its-innovation-hours-program>.
42. 15 USC § 78o-3.
43. CSBS, *Vision 2020: Fintech Industry Advisory Panel Recommendations and Next Steps* (2019), <https://www.csbs.org/sites/default/files/2019-02/FIAP%20Chart%20and%20Next%20Steps.pdf>.
44. FSB, *Fintech and Market Structure in Financial Services: Market Developments and Potential Financial Stability Implications* (Feb. 2019), <https://www.fsb.org/wp-content/uploads/P140219.pdf>; BCBS, *Implications of Fintech Developments for Banks and Bank Supervisors* (Feb. 2018), <https://www.bis.org/bcbis/publ/d431.pdf>.
45. OCC, *Press Release: OCC Begins Accepting National Bank Charter Applications From Financial Technology Companies* (July 31, 2018), <https://www.occ.gov/news-issuances/news-releases/2018/nr-occ-2018-74.html>.
46. Complaint, *CSBS v. Otting*, No. 1:18-cv-02449 (D.D.C. Oct. 25, 2018).
47. Complaint, *Vullo v. Otting*, No. 1:18-cv-08377 (S.D.N.Y. Sept. 14, 2018).
48. 328 U.S. 293 (1946).
49. *See* SEC, *Framework for "Investment Contract" Analysis of Digital Assets* (Apr. 3, 2019), https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets#_edn1 (**SEC Howey Framework**).
50. FINRA, *FINRA Forms Office of Financial Innovation, Announces Haimera Workie as Head* (Apr. 24, 2019), <https://www.finra.org/newsroom/2019/finra-forms-office-financial-innovation-announces-haimera-workie-head>.
51. CFTC, *CFTC Launches LabCFTC as Major FinTech Initiative* (May 17, 2017), <https://www.cftc.gov/PressRoom/PressReleases/pr7558-17>.

52. 12 USC § 5491(a).
53. Treasury Fintech Report, *supra* note 37, at 68.
54. NYDFS, *Press Release: DFS to Co-Host Fintech Forum with Conference of State Banking Supervisors* (Apr. 10, 2018), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1804101.
55. NYDFS, *Press Release: NYDFS BitLicense is First Comprehensive Regulatory Framework for Firms Dealing in Virtual Currency Such as Bitcoin* (Sept. 22, 2015).
56. Gertrude Chavez-Dreyfuss, *Bitstamp Granted Virtual Currency License by New York Financial Regulator*, Reuters (Apr. 9, 2019), <https://www.reuters.com/article/us-cryptocurrencies-bitlicense/bitstamp-granted-virtual-currency-license-by-new-york-financial-regulator-idUSKCN1RL1ZW>.
57. NYDFS, *Virtual Currency Business (BitLicense) Application and License Management via NMLS*, https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses/license_management.
58. *E.g.*, SEC Howey Framework, *supra* note 46; SEC, Release No. 81207, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*, at 13-16 (July 25, 2017) (**DAO Report**).
59. In the DAO investigation, the SEC found that the “reasonable expectation of profits” prong of the *Howey* test was supported by promotional materials of the issuer indicating that token purchasers would profit through the returns of the ventures to be funded by the token sales. The SEC also found that these promotional materials suggested that such returns would result from the entrepreneurial and managerial efforts of persons other than the investors, namely the issuer or others associated with it (*e.g.*, in creating successful apps or systems or selecting profitable projects for funding).
60. *See, e.g., In re Munchee Inc.*, Admin. Proc. File No. 3-18304, Securities Act Release No. 10445 (Dec. 11, 2017); DAO Report, *supra* note 55. In those cases, the SEC pointed to statements of ICO issuers – including statements in white papers related to the offering – that coin or token purchasers will profit through the returns of the venture to be funded by the coin or token sales.
61. 15 U.S.C. § 78c(a)(5).
62. Treasury Fintech Report, *supra* note 37, at 63-65.
63. *Id.* at 69.
64. Notably, the CFTC did not pursue a claim under Rule 42.2, perhaps recognising that FinCEN delegated to the CFTC only the authority to examine institutions for compliance with Bank Secrecy Act requirements and that FinCEN remains the government agency with overall authority to enforce compliance with the Bank Secrecy Act.
65. *CFTC v. IPool Ltd.*, Case No. 1:18-CV-2243 (D.D.C. Sept. 27, 2018) at para. 62 (emphasis original).
66. *CFTC v. My Big Coin Pay, Inc.*, Case No. 1:18-cv-10077-RWZ, Doc. No. 106 (D. Mass. Sept. 26, 2018).
67. *CFTC v. IPool Ltd.*, Case No. 1:18-CV-2243 (D.D.C. Sept. 27, 2018) at para. 64.

**Barbara Stettner****Tel: +1 202 683 3850 / Email: barbara.stettner@allenoverly.com**

Barbara Stettner is the managing partner of the Washington, D.C. office and a member of the firm's U.S. and global Financial Services Regulatory practices. Barbara has extensive experience representing foreign and domestic banks, asset managers, and broker-dealers on the various regulatory obligations of domestic and cross-border securities distributions and fundraising activities, including broker-dealer, investment adviser, finder and placement agent status questions, sales practice requirements, research, and the federal and state pay-to-play regulations. She regularly applies this experience in the Fintech space to various "robo adviser", "crowdfunding", and other securities distribution platforms and trading platforms employing distributed ledger technologies (or "blockchain") for ICOs and related securities sales and trading activities.

**Hilary Sunhee Seo****Tel +1 212 756 1155 / hilarysunhee.seo@allenoverly.com**

Ms. Seo brings significant expertise advising both domestic and international broker-dealers, banks, swap dealers and corporations in assessing the impact of financial regulations on their business activities and strategies. On behalf of her clients, she has advocated and obtained regulatory guidance and relief from the SEC, FINRA, CFTC and NFA. She has also guided digital asset and blockchain businesses on regulatory issues and compliance considerations.

**Jonathan Flynn****Tel +1 202 683 3858 / jonathan.flynn@allenoverly.com**

Jonathan Flynn focuses his practice on commodities, securities, derivatives and related regulatory and litigation matters. He represents a wide range of participants in the physical commodity and financial markets, including investment banks, major commodity merchants and trading houses, hedge funds and other asset managers, market intermediaries, and industry trade associations, on a broad range of regulatory issues involving the CFTC, the NFA, the SEC, and the Federal Trade Commission (FTC). Jon also represents companies and individuals in government investigations by the government regulators and the U.S. Department of Justice related to manipulation, fraud, price reporting and commodity indexes, supervisory controls, position limits, and other prohibited trade practices.

Allen & Overy LLP

1221 Avenue of the Americas, New York, NY 10020, USA

Tel: +1 212 610 6300 / URL: www.allenoverly.com

