COUNTRY COMPARATIVE GUIDES 2022

# The Legal 500 Country Comparative Guides

# United States

# FINTECH


## Contributor

Allen & Overy

**F. Dario de Martino**

M&A Partner, and Co-Head of Fintech and Blockchain | dario.demartino@allenovery.com

**Adam Chernichaw**

Technology Transactions Partner | adam.chernichaw@allenovery.com

**Barbara Stettner**

Financial Services Regulatory Partner | barbara.stettner@allenovery.com


This country-specific Q&A provides an overview of fintech laws and regulations applicable in United States.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

# UNITED STATES
# FINTECH

The authors would like to thank the invaluable contributions of Bill Satchell, Alex Touma, Dave Lewis, Brian Jebb, Wallace DeWitt, Molly Holsinger, Lena Kiely, Christine Liu, Hayde Faria, and Adele Hayer.

## 1. What are the sources of payments law in your jurisdiction?

In large part, the rules governing payments arise under State law. Insofar as payments transmitted through centralized payment systems, the basic regime is Article 4A of the Uniform Commercial Code ("**UCC**"), which has been adopted in most States. Even Fedwire Funds Service, the payment system maintained by the Federal Reserve, which constitutes the Central Bank of the United States, operates based on Regulation J of the Board of Governors of the Federal Reserve System ("**FRB**"), 12 CFR Part 210, which largely incorporates Article 4A of the UCC.

### a. *EFTA and the Remittance Guidance*

Payment having certain characteristics are also subject to the Electronic Fund Transfer Act ("**EFTA**") and the regulations (including the remittance regulations) of the Federal Bureau of Consumer Financial Protection ("**CFPB**"), thereunder (Regulation E, 12 CFR Part 1005). EFTA applies to electronic fund transfers initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer's account. [1]

The term "account" means a demand deposit (checking), savings, or other consumer asset account (other than an occasional or incidental credit balance in a credit plan) held directly or indirectly by a financial institution and established primarily for personal, family, or household purposes. 12 CFR 1005.2(b)(1). It includes a prepaid account, as defined by Regulation E. [2]

Regulation E applies to any person-to-person (P2P) or mobile payment transactions that meet the definition of EFT, including debit card, ACH, prepaid account, and other electronic transfers to or from a consumer account. [3]

A "remittance transfer" is an electronic transfer of money from a consumer in the United States to a person or business in a foreign country. It can include transfers from retail "money transmitters" as well as banks and credit unions that transfer funds through wire transfers, automated clearing house (ACH) transactions, or other methods. Under Regulation E (12 CFR 1005.30-361005.36) payment providers are generally required to give disclosures to consumers before they pay for the remittance transfers. The disclosures must contain:

- The exchange rate.
- Fees and taxes collected by the payment provider company.
- Fees charged by the company's agents abroad and intermediary institutions.
- The amount of money expected to be delivered abroad, not including certain fees charged to the recipient or foreign taxes.
- If appropriate, a disclaimer that additional fees and foreign taxes may apply.

Payment providers must also provide a receipt that reflects the information in the first disclosure or a proof of payment. The receipt must also tell a consumer the date on which the money will arrive and how the consumer can report a problem with a transfer.

### b. *FedNow Service*

The FRB is on the cusp of inaugurating its FedNow Service, which will provide real time payments on a 24/7 basis. The FedNow Service is designed for the end-to-end transfer to be completed in a matter of seconds and thus it is contemplated that the beneficiary's bank would agree that it will make funds available to the beneficiary

 

immediately after it has accepted the payment order. The target release date remains 2023 or 2024, and the FRB has said that it will announce a more specific time frame for launch, as well as earlier pilot programs, through established Reserve Bank channels. Initially, it was expected that the FedNow Service would include a transaction value limit of $25,000, with the potential to increase the limit over time. In response to recent rulemaking in which commenters observed that the $25,000 limit could inhibit use of the FedNow Service for many use cases, the FRB has agreed that the FedNow Service should support a wide variety of uses, including certain large-value transfers, and that the limit should be consistent with market practices and needs for instant payments. Therefore, before the launch of the service, the Reserve Banks will establish a transaction limit consistent with market practices and needs at the time and will announce the limit through established Reserve Bank communication channels. Recent reports suggesting the JPMorgan Chase contemplates deemphasizing the role of credit cards in favor of bank pay products speculated that the development of the FedNow Service helped to motivate its apparent change in strategy. [4]

A basic difference between the FedNow Service and the Fedwire Funds Service is that the FedNow Service will accommodate participants that choose to settle their activity over the service in their own master account (an account held by most banks participating in the Fedwire Funds Service with their own principal Federal Reserve Bank through which payments are settled and the bank deals with the Federal Reserve System) of a correspondent bank. Further, unlike the Fedwire Funds Service, which is designed to serve primarily as a large-value funds transfer system between institutional users, the FedNow Service is designed to also accommodate consumer use. Therefore, in the event that a transfer over the FedNow Service meets the definition of "electronic fund transfer" under EFTA, proposed subpart C provides that it would apply to the transfer but that EFTA would prevail to the extent of any inconsistency.

[1] 12 CFR 1005.3(b)(1) and 12 CFR 1005.3(a).

[2] 12 CFR 1005.2(b)(3).

[3] 12 CFR 1005.3(b)(1)(v); Comment 3(b)(1)-1.ii.

[4] How JPMorgan's plan to kill credit cards split the bank, Financial Times (September 23, 2022) avail. at https://www.ft.com/content/f6d8d454-2413-4f2b-945d-825d0a68730b?emailId=ee714650-3390-46d0-857c-c612be6c74d6&segmentId=8c17a373-f8ba-9470-5760-16886c284f22 .

## 2. Can payment services be provided by non-banks, and if so on what conditions?

Yes. In large part, non-bank participation in payment is subject to licensing in the states in which payment originator customers are located and the state in which the payment entity is located. Such licenses are commonly referred to as a "payment transmitter" or "money service business" licenses. Such licensees are authorized only to originate payments originating from the state(s) in which they are licensed.

a. ***ML Compliance***

Persons acting as "money transmitters" are also required to register with the Financial Crimes Enforcement Division of the U.S. Treasury ("**FinCEN**"), which is responsible for administration of the Bank Secrecy Act ("**BSA**"). [1] Under the BSA, covered financial institutions, including banks and money service businesses, are required to establish anti-money laundering ("**AML**") programs to guard against money laundering and the financing of terrorism. [2] The BSA requires that financial institutions' AML programs must include certain recordkeeping, reporting, and other requirements, such as a requirement to develop appropriate risk-based procedures for conducting ongoing customer due diligence, including ongoing monitoring to identify and report suspicious transactions. [3]

b. ***U.S. Financial Stability Oversight Council's 2022 Report on Digital Asset Financial Stability Risks and Regulation***

A recent publication by the U.S. Financial Stability Oversight Council ("**FSOC**")[4] cautions that the focus of money service business regulation on anti-money laundering controls and consumer protection largely ignores the financial stability vulnerabilities of the crypto ecosystem. It urges not only better enforcement of existing regulatory structures, but enhancement of those focused on lightly regulated spot commodity digital assets to address these concerns. Observing that the use of digital assets in payments has been inhibited by the price volatility of many digital assets, comparatively high fees, slow processing times, reliance on miners and validators, and illicit finance concerns, the FSOC Report notes that many market participants have responded by resorting to stablecoin alternatives, amplifying related activities, such as trading, lending, and borrowing. Such activities, combined with smart contracts, have facilitated the growth of "decentralized finance" ("**DeFi**"), contributing to the growth of related criminal activities [5] and amplified systemic risk. [6]

 

There are several key recommendations set forth in the FSOC Report:

- **Recommendation 1 –** FSOC recommends that its member agencies consider the following principles in their deliberations about the applicability of their current authority:
    - Same activity, same risk, same outcome;+
    - Technological neutrality;
    - Leveraging existing authority where appropriate
    - Transparency in technology
    - Addressing financial stability risks before they impair the economy
    - Monitoring mechanisms for interconnectedness
    - Prioritizing timely and orderly transaction processing and legally binding settlement
    - Facilitating price discovery and fostering market integrity
    - Obtaining, and sharing with other agencies, relevant market data
- **Recommendation 2 –** Continue to enforce existing rules and regulation.
- **Recommendation 3 –** Congress should pass legislation for the regulation of spot market for crypto assets that are not securities
- **Recommendation 4 –** Coordination among different regulators overseeing members of the same group
- **Recommendation 5 –** Congress should pass legislation creating a comprehensive prudential framework for stablecoins.
- **Recommendation 6 –** Congress should pass legislation creating a comprehensive organization-wide supervisory framework
- **Recommendation 7 –** The banking agencies should use their existing authority to review services provided to banks by crypto-asset providers and other entities in the space
- **Recommendation 8 –** Member agencies should assess the impact of vertical integration (direct market access) by retail customers on conflicts of interest and market volatility
- **Recommendation 9 –** Establish a coordinated government-wide approach to data and the analysis, monitoring, supervision, and regulation of crypto-asset activities [7]

[1] Pub. L. 91–508, codified at 12 USC 1829b and 1951–1959, and 31 USC. 5311–5329.

[2] 31 USC 5318(h)(1); 31 CFR Chapter X.

[3] 31 CFR 1020.210 and 1022.210.

[4] FSOC, Report on Digital Asset Financial Stability Risks and Regulation (October 2022) ("**FSOC Report**"), at 4-5, avail. at https://home.treasury.gov/system/files/261/FSOC-Digital-Assets-Report-2022.pdf .

[5] Chainalysis, in its 2022 Crypto Crime Report (February 2022) ("**Chainalysis 2022 Crypto Crime Report**"), avail. at https://go.chainalysis.com/2022-Crypto-Crime-Report.html , finds that the growth of crypto assets criminal activity during 2021 is significantly related to DeFi:

Two categories stand out for their growth: stolen funds and, to a lesser degree, scams. DeFi is a big part of the story for both.

* * *

Scamming revenue rose 82% in 2021 to $7.8 billion worth of cryptocurrency stolen from victims. Over $2.8bn of this total — which is nearly equal to the increase over 2020's total — came from rug pulls, a relatively new scam type in which developers build what appear to be legitimate cryptocurrency projects — meaning they do more than simply set up wallets to receive cryptocurrency for, say, fraudulent investing opportunities — before taking investors' money and disappearing. Please keep in mind as well that these figures for rug pull losses represent only the value of investors' funds that were stolen, and not losses from the DeFi tokens' subsequent loss of value following a rug pull.

* * *

We believe rug pulls are common in DeFi for two related reasons. One is the hype around the space. DeFi transaction volume has grown 912% in 2021, and the incredible returns on decentralized tokens like *Shiba Inu* have many excited to speculate on DeFi tokens. At the same time, it's very easy for those with the right technical skills to create new DeFi tokens and get them listed on exchanges, even without a code audit.

* * *

Cryptocurrency theft grew even more, with roughly $3.2 billion worth of cryptocurrency stolen in 2021 — a 516% increase compared to 2020. Roughly $2.2 billion of those funds — 72% of the 2021 total — were stolen from DeFi protocols. The increase in DeFi-related thefts represents the acceleration of a trend we identified in last year's

 

Crypto Crime report.

* * *

In 2020, just under $162 million worth of cryptocurrency was stolen from DeFi platforms, which was 31% of the year's total amount stolen. That alone represented a 335% increase over the total stolen from DeFi platforms in 2019. In 2021, that figure rose another 1,330%. In other words, as DeFi has continued to grow, so too has its issue with stolen funds. As we'll explore in more detail later in the report, most instances of theft from DeFi protocols can be traced back to errors in the smart contract code governing those protocols, which hackers exploit to steal funds, similar to the errors that allow rug pulls to occur.

Chainalysis 2022 Crypto Crime Report, at 3-6.

[6] *See, also,* President Working Group, FDIC and OCC, Interagency Report On Stablecoins (November 2021), avail. at https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf ("**PWG Stablecoin Report**"). The PWG Stablecoin Report views stablecoin as a significant potential source of systemic risk:

The potential for an individual stablecoin to scale rapidly raises three sets of policy concerns. First, a stablecoin issuer or a key participant in a stablecoin arrangement (e.g. a custodial wallet provider) could pose systemic risk – meaning that the failure or distress of that entity could adversely affect financial stability and the real economy.[26 Second], the combination of a stablecoin issuer or wallet provider and a commercial firm could lead to an excessive concentration of economic power. These policy concerns are analogous to those traditionally associated with the mixing of banking and commerce, such as advantages in accessing credit or using data to market or restrict access to products. This combination could have detrimental effects on competition and lead to market concentration in sectors of the real economy. Third, a stablecoin that becomes widely adopted as a means of payment could present concerns about anti-competitive effects, for example if users of that stablecoin face undue frictions or costs in the event they choose to switch to other payment products or services. Concerns about anti-competitive effects are thus likely to be greater absent interoperability standards for stablecoins and stablecoin arrangements.

* * *

Stablecoins also present important prudential concerns, as discussed in Part II. These prudential concerns relate to the potential for stablecoin runs, payment system risks, and the possibility that some stablecoins may rapidly scale. Because responsibilities within many of these arrangements are widely distributed, and currently fall within the jurisdiction of different regulatory agencies, or outside of the regulatory perimeter altogether, there is a risk of incomplete or fragmented oversight. Stablecoin arrangements have grown, and may continue to grow, rapidly. And as these arrangements grow, so may the risks associated with them. The recommendations presented below are focused on the prudential risks identified with respect to payment stablecoins.

PWG Stablecoin Report, at 14 and 15 (footnotes omitted).

[7] FSOC Report, at 111-118.

## 3. What are the most popular payment methods and payment instruments in your jurisdiction?

There are a variety of payment methods and instruments. Other than cash, which is making a comeback as the U.S. emerges from the pandemic lockdowns, most appear to still revolve around credit/debit cards. Payment service providers, contactless payment technology that exchange data between payment devices (e.g., mobile and POS devices) and in-app payments are usually linked to a credit/debit cards. That may change as other payment methods evolve (e.g. FedNow and payments in digital currency).

## 4. What is the status of open banking in your jurisdiction (i.e. access to banks' transaction data and push-payment functionality by third party service providers)? Is it mandated by law, if so to which entities, and what is state of implementation in practice?

Banking organizations possess a wealth of consumer data that many believe could be leveraged by third party providers for the benefit of the underlying consumers. For some time, a range of companies—many of them "fintech" companies—have been accessing consumer account data with consumers' authorization and providing services to consumers using data from the consumers' various financial accounts. Such "data aggregation"-based services include the provision of financial advice or financial management tools, the verification of accounts and transactions, the facilitation of underwriting or fraud-screening, and a range of other

 

functions. This type of consumer-authorized data access and aggregation holds the promise of improved and innovative consumer financial products and services, enhanced control for consumers over their financial lives, and increased competition in the provision of financial services to consumers.

As has been acknowledged by the CFPB, the relevant Federal regulator, there are many significant consumer protection challenges to be considered—particularly with respect to data privacy and security—as these technologies and practices continue to develop. As part of its consideration of a 2010 Congressional direction to the CFPB to "seek to implement and, where applicable, enforce Federal consumer financial law consistently for the purpose of ensuring that all consumers have access to markets for consumer financial products and services and that markets for consumer financial products and services are fair, transparent, and competitive," [1] the CFPB has carefully considered the risks and rewards of open banking.

The CFPB, while undoubtedly persuaded that consumer-authorized access and use of consumer financial account data may enable the development of innovative and improved financial products and services, increase competition in financial markets, and empower consumers to take greater control of their financial lives, remains concerned that consumers still face certain potential risks if they authorize access to consumer data, including some risks relating to the methods by which they authorize such access and by which the records are collected and used by authorized entities. The CFPB is proceeding deliberately, issuing an advance notice of proposed rulemaking in 2020, [2] and suggesting that a proposed rule is likely in late 2022. [3]

[1] 12 USC 5511 (added by Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. 111-203—July 21, 2010).

[2] CFPB, ANPR, Consumer Access to Financial Records, 85 Fed. Reg. 71003 (November 6, 2020).

[3] CFPB Rulemaking Agenda, avail. at https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202204&RIN=3170-AA78 .

## 5. How does the regulation of data in your jurisdiction impact on the provision of financial services to consumers and businesses?

Financial institutions that process payments will have strict controls on the collection, use and storage of data, driven by their obligations to their regulators. Companies in this environment who engage with the financial system in the U.S. will have to implement controls and procedures to ensure that the use and processing of customer data aligns with the regulatory landscape, as well as self regulatory organizations. These include compliance with privacy regimes such as the Gramm-Leach-Bliley privacy provisions, [1] the New York State Department of Financial Services regulations, *Cybersecurity Requirements For Financial Services Companies,* [2] the California Consumer Privacy Act,[3] the Payment Card Industry Security Standards Council PCI Data Security Standard (PCI DSS), and other consumer protection regulations at both the state or local level. In other words, there are significant compliance efforts (and associated costs) for companies looking to offer financial services and payment products to their customers.

[1] 15 USC §§ 6801-6827.

[2] 23 NYCRR 500.

[3] California Civil Code §§ 1798.100 – 1798.199.100.

## 6. What are regulators in your jurisdiction doing to encourage innovation in the financial sector? Are there any initiatives such as sandboxes, or special regulatory conditions for fintechs?

Without Federal legislation, there is little possibility of significant regulatory innovation. State action is by nature highly fragmented and, except for efforts to develop uniform frameworks, [1] has only limited capacity to deliver major innovations. The Federal banking regulators, while encouraging Federally supervised banks to be more active in providing innovative technology-based services, are also cautioning banks to more carefully manage outsourcing risk and more stringently examine banks providing "banking as a service" to would-be fintech market entrants.

The CFPB, which had earlier implemented a sandbox type initiative, has pulled back from the liberalization that such measures implied. The CFPB, commenting on such an action, stated:The Office of Competition and Innovation replaces the Office of Innovation, which opened in 2018, and Project Catalyst, launched in 2014. The Office of Innovation's primary purpose was to process applications for No Action Letters and Sandboxes that applied to an individual company's specific product offering. After a review of these programs, the [CFPB] concludes that the initiatives

 

proved to be ineffective and that some firms participating in these programs made public statements indicating that the [CFPB] had conferred benefits upon them that the [CFPB] expressly did not. [2]

The CFPB announcement focused on a significant change of direction:

The new office will support a broader initiative by the CFPB to analyze obstacles to open markets, better understand how big players are squeezing out smaller players, host incubation events, and, in general, make it easier for people to switch financial providers.

"Competition is one of the best forms of motivation. It can help companies innovate and make their products better, and their customers happier," said CFPB Director Rohit Chopra. "We will be looking at ways to clear obstacles and pave the path to help people have more options and more easily make choices that are best for their needs."

The CFPB has a statutory mandate to promote fair, transparent, and competitive markets. Families, honest businesses, and the entire economy benefit when consumer finance markets are fiercely competitive, rather than dominated by a handful of firms. Digital technology is transforming the markets, including how payments, deposits, and lending are provided and who provides them. Big banks, fintech, big tech, incumbents, and small start-ups are all jockeying to be in front. The Office of Competition and Innovation will focus on how to create market conditions where consumers have choices, the best products win, and large incumbents cannot stifle competition by exploiting their network effects or market power. [3]

Thus, the change signifies an increase in regulatory scrutiny, rather than the relaxation of rules that unduly complicate innovation or stymie entrance into a new market. Notwithstanding the CFPB's focus on new entrants and the risk that they may be strangled by incumbents, substantial regulatory momentum backs initiatives by incumbents subject to more traditional regulatory frameworks.

With encouragement from Federal banking agencies, the very largest U.S. banking organizations, including JPMorgan Chase, Bank of America, and Goldman Sachs, are spending billions of dollars annually to strengthen their ability to provide their customers with advanced services. As is described above, the Federal Reserve, operator of the Fedwire Payment Services, is launching its FedNow product which will facilitate instant payments and possibly change the competitive landscape fundamentally.

Indeed, banking regulators are also questioning some of the measures that have been used by banks—particularly smaller banks—to facilitate the entry of certain fintech firms into financial services. In particular, among smaller banks–those with total assets of less than $10bn—the regulators have identified significant "banking as a service" ("**BaaS**") partnerships between the banks and fintechs. The Federal regulators, including the CFPB, are focusing examination resources on such BaaS partnerships and there is a widespread expectation that many will be found to fall short of regulatory requirements and not to reflect the level of compliance resources ordinarily expected to be deployed by banks in managing such relationships. Thus, rather than taking steps that may facilitate such relationships, it seems likely that they regulators will instead challenge as inadequate from a compliance perspective many of the relationships currently in place.

[1] *See, e.g,* the effort of the Conference of State Bank Supervisors to establish a nationwide framework for money transmissions in the form of the Model Money Transmission Modernization Act, avail. at https://www.csbs.org/csbs-model-money-transmission-modernization-act .

[2] *See* CFPB Press Release, CFPB Launches New Effort to Promote Competition and Innovation in Consumer Finance (May 24, 2022), avail. at https://www.consumerfinance.gov/about-us/newsroom/cfpb-lauches-new-effort-to-promote-competition-and-innovation-in-consumer-finance/ .

[3] *Id.*

## 7. Do you foresee any imminent risks to the growth of the fintech market in your jurisdiction?

There are no imminent risks that could potentially impair the growth of the U.S. fintech market, but rather regulatory uncertainty for those fintech companies seeking to offer bank-like services, which could make their growth volatile.

Fintech companies that seek to provide solutions to the way traditional, bank-like consumer financial services are delivered, including online lending, investments, payments, wealth management, etc., must ensure compliance with a patchwork of state and federal laws and regulatory agencies (including, *at the federal level*: the CFPB, the Federal banking regulators, including the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency and the FRB, the securities regulator, the Securities and Exchange Commission

 

("**SEC**") and the related self-regulatory organization with responsibility for overseeing registered broker-dealers, the Financial Industry Regulatory Authority, the Commodities Futures Trading Commission ("**CFTC**"), FinCEN, and the Federal Trade Commission; and *at the state level*: state-chartered banking regulations, money transmitter laws, usury laws, data privacy and state security laws).

As a result, fintech companies must continuously develop, refine or sometimes pivot their business strategy in order to navigate a complex web of regulations and stay compliant—or face enforcement actions from regulators or law enforcement agencies.

Some fintech companies are now offering consumer banking services in collaboration with banks, which means that they may be losing part of the relationship with their customers and sharing part of the economics with banks, often as part of BaaS arrangements. Others are considering pursuing bank charters, which entails significant time and investment other than the uncertainty of the regulatory approval process.

While many fintech companies are able to thrive in the U.S., the developing regulatory framework requires careful consideration of its applicability to new business models to determine whether to pursue registration or exemption therefrom, and compliance with applicable laws and regulations.

## 8. What tax incentives exist in your jurisdiction to encourage fintech investment?

There are no fintech-specific tax credits under U.S. federal tax law. While not limited to the Fintech industry, the Internal Revenue Code provides tax credits for companies investing in research and development (**R&D**). Specifically, Section 41 of the Code [1] provides tax credits for qualified research expenses that relate to the development or improvement of any "product, process, computer software, technique, formula, or invention." Subsection 41(d)(1)(B) defines "qualified research" as research "which is undertaken for the purpose of discovering information (i) which is technological in nature, and (ii) the application of which is intended to be useful in the development of a new or improved business component of the taxpayer." Additionally, many states offer R&D tax credits at the state level, some offering lower thresholds or alternative definitions of certain terms.

[1] 26 USC 41.

## 9. Which areas of fintech are attracting investment in your jurisdiction, and at what level (Series A, Series B etc)?

The area that has continued to attract the most funding is payments, followed by crypto and DeFi, financial management solutions, wealth management, banking, mortgages and lending, insurtech, regtech, artificial intelligence and machine learning, and data analytics.

As for the level of deal stage, early-stage deal share continues to dominate in 2022 YTD, accruing about 56% of the market's operations (angel, pre-seed, seed and series A), while mid-stage investments accrue a 16%, late-stage a 10%, and the remaining 19% is found in other stages.

## 10. If a fintech entrepreneur was looking for a jurisdiction in which to begin operations, why would it choose yours?

Despite the uncertainty and complexities of the U.S. regulatory regime, the vast U.S. market continues to outpace EMEA, APAC and other jurisdictions with respect to both private and public financing, whether measured by dollar or transaction volume. According to recent industry reports, U.S. based fintech companies received $23.9bnin the aggregate from investors—representing roughly 45.1% of all total fintech investment globally.

In addition, several States (including Arizona, Florida, Nevada, Utah, West Virginia and Wyoming) have established sandboxes, which are intended to enable fintechs to test new products and services without having to obtain licenses or registrations.

Finally, California and New York are home to several fintech incubators and accelerators that offer founders support with respect to product development, sales and marketing.

## 11. Access to talent is often cited as a key issue for fintechs – are there any immigration rules in your jurisdiction which would help or hinder that access, whether in force now or imminently? For instance, are quotas systems/immigration caps in place in your jurisdiction and how are they determined?

The H-1B visa, a work visa often used by professionals in the United States, is subject to an annual numerical limitation of 65,000 visas each fiscal year, with an

 

additional 20,000 visas allocated to beneficiaries with a master's degree or higher from a U.S. university. With few exemptions available, this numerical limitation significantly restricts the ability of most U.S. employers to hire foreign nationals in the U.S., as the demand for this type of visa frequently exceeds the number of visas available each year. Some applicants may look to other temporary options such as the O-1 visa (for individuals of extraordinary ability or achievement) or the E-2 visa (for nationals of a treaty country), but many foreign nationals remain restricted by the H-1B cap.

When considering long-term options, foreign nationals also face per-country limitations for employment-based green cards, which means that many individuals wait for several years before obtaining permanent residency. While several bills have been introduced to Congress to address such limitations, no major immigration reform has occurred since 1986. In the meantime, employers will need to continue to consider creative approaches to overcome the numerical limitation challenges when hiring foreign nationals in the United States.

## 12. If there are gaps in access to talent, are regulators looking to fill these and if so how? How much impact does the fintech industry have on influencing immigration policy in your jurisdiction?

N/A

## 13. What protections can a fintech use in your jurisdiction to protect its intellectual property?

Though the traditional IP regime exists and can be leveraged to protect a company's intellectual property, one of the most significant risks to intellectual property is associated with the ubiquity of open source code in the Fintech space. Care should be taken that any code that is licensed to a Fintech company will not result in the licensee being required to publish or disclose its own proprietary code to the open source community or otherwise inadvertently relinquish its IP rights

## 14. How are cryptocurrencies treated under the regulatory framework in your jurisdiction?

**Commodities**

As an entirely new kind of property, existing independent of any legal entity issuer, and capable of being deployed to perform a wide range of functions, digital assets defy traditional categories. While they may feature elements that are seemingly characteristic of securities, commodities and a means of exchange, they are also capable of embodying creative works, performing decentralized functions and executing simple contracts.

There are compelling arguments that some digital assets constitute "commodities."

"The definition of 'commodity' in the [Commodity Exchange Act] is broad ... It can mean physical commodity, such as an agricultural product ... It can mean currency or interest rate; [Federal Commodity Futures Trading Commission ("**CFTC**")] Launches Virtual Currency Resource Web Page, Press Release, Dec. 15, 2017 ("Bitcoin and other virtual currencies have been determined to be commodities under the Commodity Exchange Act (CEA). The [CFTC] primarily regulates commodity derivatives contracts that are based on underlying commodities. While its regulatory oversight authority over commodity cash markets is limited, the CFTC maintains general anti-fraud and manipulation enforcement authority over virtual currency cash markets as a commodity in interstate commerce..

* * *

Bitcoin, Ether, Litecoin, and Tether tokens, along with other digital assets, are encompassed within the broad definition of "commodity" under Section 1a(9) of the [Commodity Exchange] Act. [1]

While the CFTC has jurisdiction over fraud in the spot market that might affect the futures and derivatives markets over which it has primary authority, it does not currently have comprehensive authority to regulate spot markets or spot market intermediaries. Hence, they are not subject to regulation under Federal law to the extent the underlying digital assets constitute "commodities."

**Securities**

To the extent what constitutes "securities," even spot sales must be effected through licensed intermediaries and are subject to a complex regulatory framework.

One might assume that the word "security" is clearly defined by U.S. law but unfortunately it is not. The definition of what constitutes a "security" found in the Securities Act of 1933 and the Securities Exchange Act of 1934 includes traditional instruments issued by legal entities, such as stocks and bonds, as well as the less familiar term "investment contract." In 1946, the Supreme Court decided *SEC v. Howey*, which gave greater substance to the meaning of this term, but little

 

that anticipated the advent of digital assets. In a case involving the ownership of orange groves combined with service contracts to cultivate and sell the resulting products. When faced with an enterprise that closely resembled a legal entity, the Supreme Court found that the sale of the orange groves together with the means by which to develop the product thereof constituted an "investment contract" and therefore a "security" within the meaning of that term under the Securities Act.

The U.S. Securities and Exchange Commission ("**SEC**"), the agency responsible for oversight with respect to the Securities Act, has applied the *Howey* test [2] to conclude that the resulting digital assets themselves are securities. Typically, a developer issues digital assets or the right to acquire digital assets to fund the further development of the underlying assets and typically the platforms through which they will trade. While that schema undoubtedly constitutes an investment contract, many have argued that the SEC's conclusion that the resulting digital assets are securities is rather like concluding that oranges from the *Howey* groves constituted securities. This argument, however, is an overly-narrow interpretation of the existing Howey test. In Howey, the Supreme Court recognized the need to scrutinize the arrangement in totality, rather than the assets that underlie such arrangement, to determine whether it was an investment contract. The key term is "investment contract," and the inclusion of the word "contract" means that there must be an arrangement whereby there is an investment of money with the expectation of making a profit, in a common enterprise, *derived from the efforts of others*, i.e. not every product of an investment contract should be deemed a security. Such digital assets represent no ownership of a business and no claim on the revenues, income or assets of the resulting enterprise, although their existence and functionality may have benefitted from the work of the enterprise.

The analytical challenge is aggravated because the Securities Act (and the related Securities Exchange Act of 1934) are all premised on the assumption that all securities are issued by legal entities. The result is that if tokens are "securities" there is no obvious path to regularizing trading of such interests. While the SEC has suggested that it may look at how to regularize digital assets that are not securities, to date it has provided no meaningful guidance.

If we continue to apply the Howey test, and the related framework, to any asset produced by the subject arrangements or enterprise, then we would need to apply it to other things, such as frequent flyer miles, loyalty points, etc., which would lead to indefensible results.

The SEC even published a detailed framework for how to determine an investment contract in the context of digital assets in 2019.[3] While the SEC's 2019 framework was helpful guidance, it created a test under which both the enterprise to cultivate oranges and the resulting oranges would likely be deemed securities.

Interestingly, the SEC staff has determined that only two truly decentralized cryptocurrencies, bitcoin and (albeit with some less enthusiasm) ether, are not investment contracts and therefore not securities. In making this determination, the SEC staff emphasized the importance of decentralization in determining whether a token should be considered a security, stating "[i]f the network on which the token or coin is to function is sufficiently decentralized—where purchasers would no longer reasonably expect a person or group to carry out essential managerial or entrepreneurial efforts—the assets may not represent an investment contract."

However, no helpful guidance has been offered to define or achieve "sufficient decentralization", leaving market participants in a conundrum.

There is increasing discussion of legislative action in this area which might distinguish between the promotion of schemes to develop digital assets and the resulting digital assets (provided that they do not independently represent third party obligations). There is also the possibility that the Court might resolve the quandary, but it is difficult to discern the ultimate path out of the current uncertainty. The urgency of such measures is amplified by the failure of several intermediaries of the resulting harm to market participants from the lack of regulatory clarity. While the SEC might be heard to argue that this results from the refusal to acknowledge the character of many digital assets as securities, its interventions in the markets have been neither constructive nor laid out a clear path that reflects the very different characteristic of many digital assets from securities.

[1] *CFTC v. McDonnell*, 287 F. Supp. 3d 213, 226 (E.D.N.Y 2018) ("Virtual currencies can be regulated by CFTC as a commodity."), *mot. for reconsideration denied*, 321 F. Supp. 3d 366 (E.D.N.Y. 2018).

[2] In *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946), the Court established a four-point test in determining whether a financial asset constitutes an "investment contract" and thus is a security:

1. An investment of money;
2. In a common enterprise;
    a. In the view of the SEC, investments in digital assets constitute investments in a "common

 

enterprise" because the fortunes of digital asset purchasers are linked to each other or to the success of the promoter's efforts.

3. With the expectation of profit; and
    a. The digital asset gives the holder rights to share in the enterprise's income or profits or to realize gain from capital appreciation of the digital asset.
        i. The opportunity may result from appreciation in the value of the digital asset that comes, at least in part, from the operation, promotion, improvement, or other positive developments in the network, particularly if there is a secondary trading market that enables digital asset holders to resell their digital assets and realize gains.
        ii. This also can be the case where the digital asset gives the holder rights to dividends or distributions.
    b. The digital asset is transferable or traded on or through a secondary market or platform, or is expected to be in the future.
4. To be derived from the efforts of others.
    a. Does the purchaser reasonably expect to rely on the efforts of a promoter or manager?
    b. Are those efforts "the undeniably significant ones, those essential managerial efforts which affect the failure or success of the enterprise," as opposed to efforts that are more ministerial in nature?

[3] SEC, Framework for "Investment Contract" Analysis of Digital Assets (April 23, 2019), avail. at https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets /

## 15. How are initial coin offerings treated in your jurisdiction? Do you foresee any change in this over the next 12-24 months?

To the extent that initial coin offerings evidence the promotional features underlying the *Howey* test described above (and most do), the resulting transactions would be characterized as securities. Absent legislative solutions or definitive case law, no change is presently foreseeable.

## 16. Are you aware of any live blockchain projects (beyond proof of concept) in your jurisdiction and if so in what areas?

N/A

## 17. To what extent are you aware of artificial intelligence already being used in the financial sector in your jurisdiction, and do you think regulation will impede or encourage its further use?

Artificial intelligence ("**AI**") models become increasingly large and complex, having been trained on ever-growing datasets, and deployed across a variety of use cases. Among others, companies have continued to use AI in connection with fraud detection, cybersecurity, customer behavioral analytics and chatbots to address customer queries. In addition, AI is being used in connection with underwriting loans, managing risk and compliance with fair-lending requirements. The latter, however, has been criticized as AI may discriminate according to certain underlying factors such as sex, age, race or origin (among others), which may lead to a biased automated lending system. To tackle the way these unfair uses and other potential risks for AI, the Algorithmic Accountability Act of 2022 [1] was introduced in both houses of Congress in February 2022 and is still pending approval. This act, if passed, would direct the FTC to create regulations that mandate businesses to meet certain criteria and provide impact assessment mechanisms when using automated decision-making processes such as AI and Machine Learning

Despite the above, most AI operations remain limited in their scope and scale within companies. Additionally, companies have become focused on cloud computing costs during the current period of economic volatility and have sought cost efficiencies in their AI infrastructure, for example shifting spending to on-premises and edge AI chips.

In the U.S., regulation of AI is fragmented, with laws being enacted at both state and federal levels. This legislative patchwork can make it difficult for companies leveraging (or attempting to leverage) AI to remain compliant. We believe a more unified approach to AI regulation—both nationally and internationally—can

 

strengthen oversight as well as promote development. Of course, this will be challenging as AI can be trained and deployed in a multiple of ways.

The principal U.S. financial regulation agencies, by means of a request for comment in March 2021, [2] acknowledged that they support innovation by financial institutions so long as accompanied by a robust identification and management of risks associated with the use of new technologies and techniques. In view of such agencies, with appropriate governance, risk management, and compliance management, financial institutions' use of innovative technologies and techniques, such as those involving AI, has the potential to augment business decision-making and enhance services available to consumers and businesses. In the request for comment, the agencies identify some of the likely uses of such technologies:

- *Flagging unusual transactions*. This involves employing AI to identify potentially suspicious, anomalous, or outlier transactions (e.g. fraud detection and financial crime monitoring).
- *Personalization of customer services*. AI technologies, such as voice recognition and natural language processing, are used to improve customer experience and to gain efficiencies in the allocation of financial institution resources.
- *Credit decisions*. This involves the use of AI to inform credit decisions in order to enhance or supplement existing techniques.
- *Risk management*. AI may be used to augment risk management and control practices.
- *Textual analysis*. Textual analysis refers to the use of natural language processing for handling unstructured data (generally text) and obtaining insights from that data or improving efficiency of existing processes.
- *Cybersecurity*. AI may be used to detect threats and malicious activity, reveal attackers, identify compromised systems, and support threat mitigation.

The agencies note that many of the potential risks associated with using AI are not unique to AI, pointing out that the use of AI could result in operational vulnerabilities, cyber threats, information technology lapses, risks associated with the use of third parties, and model risk, all of which could adversely affect a financial institution's safety and soundness. Equally, the agencies are focused on the risk that the use of AI may create or heighten consumer protection risks, such as risks of unlawful discrimination, unfair, deceptive, or abusive acts or practices ("**UDAAP**"), [3] unfair or deceptive acts or practices ("**UDAP**"), [4] or privacy concerns. [5]

One of the areas that has probably garnered the greatest attention is the risk of employing AI in connection with credit underwriting, and particularly the risk that an AI solution will, in a way that is not transparent or immediately perceptible, discriminate against a potential borrower in a way that violates Federal anti-discrimination laws, including the Fair Credit Reporting Act ("**FCRA**") and CFPB Regulation V thereunder, [6] the Equal Credit Opportunity Act ("**ECOA**") and CFPB Regulation B thereunder, [7] and the Fair Housing Act ("**FHA**").

Guidance given by the CFPB in May 2022 exemplifies the complications of relying on AI in the credit context. [8] ECOA and Regulation B require prospective lenders ("**creditors**") to provide statements of specific reasons to applicants for credit against whom there is: (i) a refusal to grant credit in substantially the amount or on substantially the terms requested in an application unless the creditor makes a counteroffer (to grant credit in a different amount or on other terms) and the applicant uses or expressly accepts the credit offered; (ii) a termination of an account or an unfavorable change in the terms of an account that does not affect all or substantially all of a class of the creditor's accounts; or (iii) a refusal to increase the amount of credit available to an applicant who has made an application for an increase (each, an "**adverse action**").

Some creditors may make credit decisions based on certain complex algorithms, sometimes referred to as uninterpretable or "black-box" models, that make it difficult—if not impossible—to accurately identify the specific reasons for denying credit or taking other adverse actions. The requirement that a creditor gives an applicant specific notice of an adverse action notice in accordance with ECOA and Regulation B, however, apply equally to all credit decisions, regardless of the technology used to make them. Thus, ECOA and Regulation B do not permit creditors to use complex algorithms when doing so, which means they cannot provide the specific and accurate reasons for adverse actions.

Regulation B explains that "[s]tatements that the adverse action was based on the creditor's internal standards or policies or that the applicant, joint applicant, or similar party failed to achieve a qualifying score on the creditor's credit scoring system are insufficient." The Official Interpretations to Regulation B explain that "[t]he specific reasons disclosed … must relate to and accurately describe the factors actually considered or scored by a creditor."

Accordingly, creditors must be able to provide applicants

 

against whom adverse action is taken with an accurate statement of reasons. The statement of reasons "must be specific and indicate the principal reason(s) for the adverse action." [9]

[1] H. R. 6580, avail. at https://www.congress.gov/bill/117th-congress/house-bill/6580/text#:~:text=To%20direct%20the%20Federal%20Trade,Algorithmic%20Accountability%20Act%20of%202022%E2%80%9D.

[2] CFPB, FDIC, FRB, NCUA, OCC, Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning, 86 Fed. Reg. 16837 (March 31, 2021) ("**Agency AI Request for Information**").

[3] Specifically relating to the CFPB's authority under 12 USC 5531.

[4] Under Section 5 of the Federal Trade Commission Act, 15 USC 45.

[5] Agency AI Request for Information, 86 Fed. Reg. at 16839.

[6] 15 USC §§ 1681-1681x and CFPB Regulation V thereunder, 12 CFR Part 1022.

[7] 15 USC §§ 1691-1691f and CFPB Regulation B thereunder, 12 CFR Part 1002.

[8] CFPB Circular 2022-03, Adverse action notification requirements in connection with credit decisions based on complex algorithms (May 26, 2022) ("**CFPB Circular 2022-03**"), avail. at https://files.consumerfinance.gov/f/documents/cfpb_2022-03_circular_2022-05.pdf .

[9] CFPB Circular 2022-03, at 3.

## 18. Insurtech is generally thought to be developing but some way behind other areas of fintech such as payments. Is there much insurtech business in your jurisdiction and if so what form does it generally take?

Insurtech funding in the U.S. has amounted to $4.8bn across 288 deals in 2022 YTD. Despite this being at 28% of the 2021 record, the U.S.'s insurtech market grows steadily while retaining 46% of the global deal share in this industry.

Among the areas in which insurtech is thriving, the main trend taking place in the U.S. is partnerships between insurance companies and insurtechs. What once was a rivalry between the traditional insurance companies and the new technological solutions, has shifted towards a partnership system where both can benefit from each other. Large insurance companies are either purchasing or entering into partnerships with insurtech companies to provide their clients with more personalized and innovative products. Insurtechs seek to deliver better customer experiences and efficiencies through data-driven insights that shape the customer's digital journey. AI, big data, cCloud and embedded insurance are the main four technology solutions that are proving themselves trendy and effective among the main insurtech providers.

In addition, insurtech startups that have incorporated emerging technologies, such as cloud, predictive analytics, telematics and application programming interfaces have fared better in the market. They have benefited from increased data accessibility and have been successful in expanding into new markets, including cyber risk. For example, this past June, Coalition, a San Francisco-based startup that combines cyber insurance and proactive cybersecurity tools, raised a $250m Series F investment backed by Allianz X, Valor Equity Partners and Kinetic Partners Management. We expect that insurtech startups with disruptive solutions will continue to find opportunities in the market, whereas large incumbents will continue to experience slow growth.

## 19. Are there any areas of fintech that are particularly strong in your jurisdiction?

The transformation of financial services toward digitization, seamless global integration and online channels has accelerated over the past year, benefiting the growing ecosystem of fintech companies that seek to address shortfalls and gaps in the traditional markets and take advantage of the opportunities generated by new technologies and innovation.

The U.S. continues to be at the forefront of this transformation and remains a fintech stronghold across several sub-sectors, specifically with respect to the provision of third party banking services, consumer/personal finance, payments, digital assets, lending, financial education and literacy, financial advisory and robo-advisory services.

## 20. What is the status of collaboration vs disruption in your jurisdiction as between fintechs and incumbent financial

 

### institutions?

While fintech companies who seek to disrupt traditional financial institutions remain (for example, by providing high-return crypto savings accounts—not without significant risks), collaboration has become the most common model to operate in this market (see, for example, MasterCard's strategic relationship with payment technology platform Global Processing Services, or the collaboration between Cross River Bank and Affirm, where Affirm provides buy-now, pay-later offerings, while Cross River provides a compliance and back-end infrastructure).

In addition, financial institutions are actively seeking to adopt and leverage financial technology either by acquiring fintechs (for example, Visa's attempted acquisition of Plaid in 2020), or to a lesser extent by creating their own technologies (such as digital payments network Zelle, which is owned by seven U.S. banks).

### 21. To what extent are the banks and other incumbent financial institutions in your jurisdiction carrying out their own fintech development / innovation programmes?

Banks and financial institutions in the U.S. are active in fostering relationships with early-stage companies in this space.

Some incumbents are also expanding their venture capital arms to focus on fintech investments or, to a lesser extent, create their own accelerators and incubators.

### 22. Are there any strong examples of disruption through fintech in your jurisdiction?

Over the past year, the fintech industry has grown exponentially in the U.S., reshaping traditional markets and customer expectations and demand for financial products and services, providing new opportunities for investors while driving innovation into virtual banking, cloud-based lending, and all forms of digital payments and digital finance. Fintech is now a ubiquitous and seamless aspect of the retail consumer and retail banking experience in the U.S. For example, while about 30% of adults in the U.S. used a mobile wallet before the pandemic, that percentage increased to 68% in 2021. Even brick-and-mortar retail stores utilize mobile payment fintechs such as Stripe and Plaid to process payments.
Innovation in financial technology is also creating significant challenges for traditional industry leaders and unique opportunities for new entrants. For example, such entrants include "TechFins," which are the technology companies who embed financial services to make their own products more attractive but whose business model does not depend on margin in those financial services.

Some commentators forecast that one in two smartphone owners in the U.S. will use proximity mobile payments (e.g. Apple Pay) by 2025, as people turn to mobile wallets in search of contactless ways to pay in-store. As the trend progresses, wallet providers will be looking beyond the low-hanging fruit to hook future—and possibly less eager—adopters by increasing the ancillary products and services available through mobile wallets.

These industry tailwinds are expected to continue driving investment capital into fintech companies across both the private and public markets.

## Contributors

**F. Dario de Martino**
**M&A Partner, and Co-Head of Fintech and Blockchain**
dario.demartino@allenovery.com

**Adam Chernichaw**
**Technology Transactions Partner**
adam.chernichaw@allenovery.com

**Barbara Stettner**
**Financial Services Regulatory Partner**
barbara.stettner@allenovery.com