Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches

Tracy French

Barbara Stettner

Allen & Overy LLP

Note

This article first appeared in the April 2018 edition of the ICLG to: Anti-Money Laundering. Below the entire article has been reproduced and updated to reflect the current state of anti-money laundering regulation of cryptocurrency in the United States and in selected jurisdictions across the globe.

Introduction

In recent years, cryptocurrencies[1] have emerged as a prominent feature of the global financial system. Since the first decentralised cryptocurrency, Bitcoin, was unveiled by the mysterious figure known only as "Satoshi Nakamoto" in 2009,[2] both the overall value of cryptocurrency in circulation and the variety of different types of cryptocurrency have expanded dramatically. According to one estimate, the global market capitalisation of cryptocurrencies exceeded USD602 billion in the fourth quarter of 2017, before falling below USD300 billion in 2018.[3]

Due to this growth, cryptocurrencies and initial coin offerings ("**ICOs**") have become an important form of personal wealth and a broad range of cryptocurrency-related businesses have emerged to serve the cryptocurrency sector. These include businesses that are directly involved in cryptocurrency trading and development, such as cryptocurrency exchanges and cryptocurrency "mining" operations,[4] as well as those that provide ancillary services to or are otherwise indirectly involved with the cryptocurrency markets and participants, including, but not limited to, firms in the retail, banking, gaming, and computing sectors. The growth of such markets has been fuelled by substantial investor interest, such that many now include cryptocurrencies within their investment portfolios.

For regulated financial institutions ("**FIs**"),[5] the opportunities presented by cryptocurrencies and distributed ledger technology ("**DLT**")[6] are tied to significant operational and regulatory challenges, not least to the implementation of anti-money laundering and counter-terrorist financing (together, "**AML**") regimes. From the regulatory standpoint, many of the risks associated with cryptocurrencies echo those presented by new financial products and technologies of the past: the risk of untested business models; the potential for abuse and fraud; the lack of a clear and shared understanding of DLT and how cryptocurrencies are sold and traded over it; and the related uncertainty of a still unshaped regulatory environment.

At the same time, key aspects of the cryptocurrency ecosystem are, by design, different from past internet-based systems and platforms. Peer-to-peer transaction authentication was created to permit coin holders to bypass institutional intermediaries, who are required to serve as essential gatekeepers in the global AML regime and in the broader financial markets. The potential for mutual anonymity among counterparties can frustrate the Know-Your-Customer ("**KYC**") and customer identification procedures ("**CIP**") on which existing AML regimes depend. The online ecosystem surrounding cryptocurrency opens new cyber and insider threat vulnerabilities, while the iterative nature of the DLT underlying cryptocurrencies prevents reversibility when a fraudulent or unlawful transaction has occurred. Finally, the absence of in-built geographic limitations makes it difficult to resolve which jurisdiction, or jurisdictions, may potentially regulate each underlying activity.

In this environment, both FIs and regulators must confront technically complex problems in a compressed time-span and in the face of what often appear to be unquantifiable risks. After an initial period of relative forbearance, financial regulators are now responding more aggressively to emerging risks and potential benefits associated with cryptocurrency, ICOs, and DLT. Recent moves by regulators in the United States and other jurisdictions to assert authority over cryptocurrency markets underscore this backdrop of legal and regulatory uncertainty. The ambiguous legal status of many cryptocurrency businesses further raises the stakes for FIs doing business with cryptocurrency entrepreneurs, whose regulatory risk tolerance may be more likely to reflect the 'wild west' culture of technology startups than that of traditional financial services providers.

Acknowledging the dynamism of the present moment, this chapter seeks to provide a high-level view of how the emerging cryptocurrency sector intersects with AML regulations and the risk-based AML diligence systems maintained by FIs. To begin, section 2 provides a brief description of how cryptocurrencies function, including the underlying technology and associated cryptocurrency businesses. Section 3 presents a non-exhaustive survey of the evolving regulation of cryptocurrency in key jurisdictions, with an emphasis on major financial centres and contrasting approaches to cryptocurrency AML regulation. Finally, section 4 identifies cryptocurrency risk considerations for FIs, focusing on risks posed by customers who hold, produce, or otherwise interact with cryptocurrencies to a significant degree and by services provided to cryptocurrency markets.

Cryptocurrency Overview

Before outlining how governments have applied AML rules to cryptocurrencies, it is helpful to establish both a basic technical understanding of how cryptocurrencies work and a common vocabulary for the types of products, services, and actors that play a role in the cryptocurrency markets.

Key Terms

Cryptocurrency is a form of virtual currency. FATF has defined "**virtual currency**" as "a digital representation of value" that "does not have legal tender status ... in any jurisdiction", and serves one or more of three functions: (1) "a medium of exchange"; (2) a "unit of account"; or (3) "a store of value".[7] Lack of legal national tender status is what, under the FATF definition, distinguishes virtual currency from "**fiat currency**", which is traditional national currency, and "e-money", which is a digital representation of fiat currency. Virtual currencies may be either convertible[8] (having a fixed or floating equivalent value in fiat currency) or non-convertible[9] (having use only within a particular domain, such as a game or a customer reward programme), and the administration of a virtual currency may be centralised[10] (controlled by a single administrator) or decentralised (governed by software using DLT principles).[11]

Under this taxonomy, a paradigmatic cryptocurrency such as Bitcoin is a convertible, decentralised virtual currency that "utilizes cryptographic principles" to ensure transactional integrity, despite the absence of trusted intermediaries such as banks. While Bitcoin, which launched in early 2009, is the oldest and most well-known cryptocurrency, many variations have since been created with various features. LiteCoin, the second-longest running cryptocurrency after Bitcoin, used the same source code but permits more efficient decryption (also known as "hashing" or "mining," as discussed below). Ether, which as of this writing has the second largest market cap after Bitcoin, debuted in 2015 and is built on a flexible "smart contract" protocol called Ethereum, which can in turn be used to encode rights in a variety of asset types into a DLT-tradable form.[12] More recent variants, such as Ripple, provide for issuance and redemption through a centralised administration controlled by a consortium of banks, while retaining decentralised exchange based on an encrypted ledger for transactions. The most recent boom has seen cryptocurrency increasingly adopted as a means of raising capital, often portrayed as a variant of "crowdsourcing" startup costs. As noted below, however, the use of cryptocurrencies to raise capital for investment purposes can raise issues under applicable securities laws and other financial regulatory regimes. Depending on the technical structure of the cryptocurrency issued, some issuers and related persons point to "utility characteristics" of the cryptocurrency (sometimes called a "coin" or "token") to argue that it is not a security under relevant case law discussed below. However, SEC Chairman Jay Clayton has cautioned that many such assertions "elevate form over substance" and that structuring a coin or token to provide some utility does not preclude it from being a security. Indeed, Chairman Clayton emphasises that a token or coin offering has the hallmarks of a security under U.S. law if it relies on marketing efforts that highlight the possibility of profits based on the entrepreneurial or managerial efforts of others, regardless of structure.[13]

Blockchain Technology

Technologically speaking, cryptocurrencies such as Bitcoin operate on the basis of a global transaction record known as a "**blockchain**". A variety of resources are available to help explain blockchain technology more thoroughly than can be done here.[14] However, at a high level, a blockchain is a particular form of DLT that requires the resolution of a new, randomised cryptographic key in order to be updated with more recent transfers. Each successive key is resolved through a process known as "**hashing**", which in practice is achieved through the ongoing computational guesswork of all computers in the network until one of the computers identifies the correct key, thus decrypting the latest iteration of the ledger (and, in the case of Bitcoin and cryptocurrencies that follow a similar model, releasing a small amount of new cryptocurrency into the world by means of a payment to the "miner" with the correct hash). Each time this occurs, the validated block of new transactions is timestamped and added to the existing chain in a chronological order, resulting in a linear succession that documents every transaction made in the history of that blockchain. Rather than residing in a centralised authoritative system, the blockchain is stored jointly by every computer node in the network. This distributed, encrypted record is what provides assurance to mutually anonymous, peer-to-peer transferees that there can be no double-spending, despite the absence of a trusted intermediary or guarantor.[15]

Blockchain has been described as "anonymous, but not private".[16] The anonymity (or "pseudo-anonymity")[17] of blockchain derives from the fact that a party transacting on the ledger is identified only by a blockchain address, which acts as an account from which value can be sent and received and can in principle be created without providing personal identifiable information. On the other hand, blockchain is not "private", since all transactions on the ledger are a matter of public record and every coin is associated with a unique transaction history. Complicating this picture, users with an interest in secrecy can employ a variety of technical tools to obscure the relationship between different blockchain addresses and actual transacting parties – while, as a countermeasure, increasingly complex data analytics methods are being developed that can identify related blockchain transactions and attribute addresses to particular users under certain circumstances.[18] The fact that even well-resourced and technically sophisticated actors face limits on their ability to decipher blockchain transactional activity, however, makes cryptocurrency attractive for money launderers and other parties seeking to exchange value away from the formal financial sector.

Cryptocurrency Businesses

Creation of a new cryptocurrency requires the development and release of the software that establishes the rules for its use, maintains the ledger, and governs the issuance and redemption of the cryptocurrency.

FATF defines a person or entity engaged as a business in putting a virtual currency into circulation and who "has the authority to redeem…the virtual currency" as the "**administrator**" of the virtual currency.[19] Many cryptocurrencies – including some of the most significant examples, such as Bitcoin, Litecoin, and Ether – have no administrator. Such cryptocurrencies are run on open-source software that governs issuance and redemption, and no central party has authority to modify the software or the rules of exchange. Other DLT applications have been developed that use the distributed ledger for validating transfers while retaining central control over issuance and redemption. The result is that the universe of "cryptocurrencies" encompasses a diverse range of virtual currencies, "coins", and "tokens" that have varying uses and characteristics and that are subject to very different degrees of control by their operators.

In addition to the creators and administrators of cryptocurrency, supporting applications have been developed to ease access and use of the underlying peer-to-peer system. In particular:

- A **Virtual Wallet** ("**wallet**") is a software application or other mechanism for holding, storing and transferring virtual currency.
  - *Custodial versus Non-Custodial*: A custodial wallet is one in which the virtual currency is held by a third party on the owner's behalf, whereas a non-custodial wallet is one in which the virtual currency owner holds his own private keys and takes responsibility for the virtual currency funds himself.

- *Hot versus Cold*: Wallet storage may be "cold", meaning held offline (usually on a USB drive) and plugged in only when needed, or "hot", meaning held online (e.g., in one of many crypto wallet applications).

- A **Virtual Currency Exchange** ("**VCE**") is a trading platform that, for a fee, supports the exchange of virtual currency for fiat currency, other forms of virtual currency or other stores of value (for example, precious metals). Individuals may use exchangers to deposit and withdraw money from trading accounts held by the VCE or to facilitate crypto-to-crypto and crypto-to-fiat exchange with the VCE or third parties through the VCE.

Whereas individual blockchain account holders may not need to involve a bank in order to obtain and transfer cryptocurrency value, the operators of these platforms frequently require traditional financial services to facilitate exchange, banking, financing, and investment with the non-crypto economy. And because the operators of these platforms typically seek to serve a large community of cryptocurrency holders for profit, they confront many of the same money laundering, fraud, cyber, and sanctions vulnerabilities as traditional financial institutions. And while the leading wallet and VCE providers use centralised data and processing models,[20] new efforts to decentralise cryptocurrency storage and exchange services create further complexity.[21] Adding to the risks, many wallet and VCE providers may, correctly or incorrectly, consider their businesses to fall outside the scope of existing AML regulations. Going forward, how to apply existing AML regimes to this complex and rapidly changing ecosystem will be a critical question for financial crime regulators.

State of Global AML Regulation

In recognition of the calls for the adoption of global AML standards for cryptocurrency trading,[22] FATF announced that it has finalised and will formally adopt as part of the FATF standards in June 2019 an Interpretive Note to Recommendation 15 to clarify how the FATF standards apply to activities or operations involving virtual assets. This should serve to reinforce what is emerging as the leading view that cryptocurrency payment service providers should be subject to the same obligations as their non-crypto counterparts,[23] and the majority of jurisdictions that have issued rules or guidance on the matter have concluded that the commercial exchange of cryptocurrency for fiat currency (including through VCEs) should be subject to AML obligations (or, in the case of China, prohibited). Salient differences in national regulations include: (i) the existence of special licensing requirements for VCEs; (ii) the extent to which AML rules also cover administrators and wallet services; (iii) the extent to which ICOs are covered by securities laws or equivalent regulations with AML regulatory implications; and (iv) the extent to which crypto-to-crypto exchange is treated differently from crypto-to-fiat exchange. As discussed below, in many cases the regulatory status of these activities is either ambiguous or case-specific, or is otherwise subject to pending changes in law and regulation. Note that while national security sanctions laws are outside of the scope of this article, the breadth of sanctions screening requirements will generally be equal and, more often, exceed that of AML compliance obligations.

U.S. Regulatory Approach

For purposes of U.S. federal law, a given cryptocurrency may variously be considered a currency, a security, or a commodity (and potentially more than one of these at once) under overlapping U.S. regulatory regimes. Whether particular activities involving that cryptocurrency are subject to AML regulatory obligations depends on whether the person engaging in these activities, by virtue of doing so, falls within one of the categories of "financial institutions" designated pursuant to the U.S. Bank Secrecy Act ("**BSA**").[24] The definition of "financial institution"[25] depends, *inter alia*, on registration requirements imposed by the Financial Crimes Enforcement Network ("**FinCEN**") (with respect to "money services businesses"),[26] the Securities and Exchange Commission ("**SEC**") (with respect to issuers, brokers, and dealers of securities),[27] and the Commodity Futures Trading Commission ("**CFTC**") (with respect to brokers and dealers of commodities and related financial derivatives).[28] While the regulatory framework is still emerging, these classifications potentially extend AML rules to most or all VCEs and to many cryptocurrency issuers and wallet providers. Moreover, while beyond the scope of this chapter, states can and increasingly do apply their own licensing and regulatory requirements, such as the New York State Department of Financial Services "Bitlicense" regulation.[29]

(a) Cryptocurrency Activities Triggering "Financial Institution" Status

The framework for cryptocurrency AML regulation in the U.S. is most developed for centralised VCEs. In 2013, FinCEN issued guidance concluding that "virtual currency" is a form of "value that substitutes for currency",[30] and that certain persons administering, exchanging, or using virtual currencies therefore qualify as money services businesses ("**MSB**")[31] regulated under the Bank Secrecy Act.[32] In doing so, FinCEN distinguished those who merely use "virtual currency to purchase goods or services"[33] (a "user") from exchangers and administrators of virtual currency,[34] concluding that the latter two qualify as MSBs unless an exemption applies.[35] In both cases, such a business qualifies as a covered MSB if it "(1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason".[36] FinCEN has clarified in subsequent administrative rulings that this definition was not intended to cover companies' buying and selling cryptocurrencies for their own use or software developers that do not also operate exchanges.[37] The extent to which a software developer that creates the cryptocurrency that it then sells directly to users (for example, as an ICO) falls within the MSB definitions remains uncertain.[38]

Separately from FinCEN's MSB regulations, the SEC regulates transactions in securities, including by requiring issuers to register offerings of securities or to rely on an available exemption from registration. The definition of "security" under the Securities Act is extremely broad.[39] Certain tokens, including those that are effectively digital representations of traditional equity interests or debt (such as partnership interests, limited liability company interests or bonds), are plainly securities under the Securities Act. The characterisation of other tokens as securities or non-securities may be less obvious. Whether a particular instrument may be characterised as an "investment contract", and therefore a "security", is the subject of decades of SEC and SEC staff guidance, enforcement matters, and case law. In the ICO context, recent SEC speeches[40] and guidance[41] have underscored that the SEC continues to apply the analysis laid out in *SEC v. W.J. Howey Co.*[42] and the cases that followed it, specifically, 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".[43] Since first invoking this view in its investigation of the DAO ICO,[44] the SEC has taken the view that several ICOs constituted offerings of securities that failed to comply with the registration requirements of Section 5 of the Securities Act of 1933 ("**Securities Act**").[45]

While acting as a securities issuer does not make the issuer a "financial institution" under the BSA, the obligation to register a cryptocurrency as a security entails a number of Securities Act obligations,[46] and the default anonymity of cryptocurrency holders may preclude ICOs from relying on common exemptions from securities registration.[47] Furthermore, if the token offered in an ICO is deemed a security, a party that transmits tokens to purchasers on behalf of issuers or other sellers could become a securities broker-dealer for purposes of the Securities Exchange Act of 1934 (the "**Exchange Act**")[48] and accordingly be required to register as a broker-dealer subject to BSA FI obligations.[49] Similarly, when the cryptocurrencies traded are, or should be, registered as securities, a VCE may be acting as a dealer (if it acts as a market-maker for trading parties) or as a broker (a person that is in the business of effecting transactions in a cryptocurrency on behalf of others),[50] and would thus be acting as a covered FI for purposes of the BSA, absent an applicable exemption.[51]

In 2014, the CFTC observed that cryptocurrencies may constitute "commodities" under the Commodity Exchange Act ("**CEA**"), such that the CFTC has broad jurisdiction over derivatives that reference cryptocurrencies (e.g., futures, options, and swaps) and market participants that transact in such contracts. In addition, under its enforcement authority, the CFTC has asserted authority to pursue suspected fraud or manipulation with respect to the cryptocurrency itself,[52] an authority recently affirmed in federal court.[53] Persons that act as futures commission merchants ("**FCM**")[54] or introducing brokers[55] ("**IBs**") for cryptocurrency derivatives under the CEA are also covered by BSA AML requirements.[56]

(b) Consequences of Coverage

Slightly different AML programme and reporting requirements, among other things, may apply under the BSA, depending on the particular class of FI involved. However, whether qualifying as an MSB or a broker or dealer in securities or commodities, the BSA requires an FI to maintain a risk-based AML compliance programme, apply CIP, report suspicious activity and certain other transactions, and maintain certain records.[57] MSBs are further required to register with FinCEN[58] (in contrast to brokers and dealers in securities or commodities, who register with their respective regulators) and in the states where they operate, as applicable, and are subject to lower SAR filing thresholds.[59] Though the transmission of funds by MSBs does not necessarily result in the creation of a customer relationship for purposes of AML regulation, MSBs are nonetheless required to obtain identification and retain records when handling transfers of USD3,000 or more.[60] Similarly, while Currency Transaction Reporting ("**CTR**") requirements do not apply to cryptocurrency-to-cryptocurrency exchange, transactions that involve cash or equivalents for cryptocurrency would be required to be reported under these rules, including obtaining identification of the individual presenting the transaction and any person on whose behalf the transaction is made.[61]

Because FinCEN's definition of MSBs excludes registered securities and commodities brokers and dealers, the requirements specific to registered brokers and dealers prevail where cryptocurrency activities would support coverage under either prong.[62] In addition to the programmatic, reporting, and record-keeping requirements referenced above, the technical characteristics of virtual currencies could also complicate U.S. broker-dealers' efforts to fulfil their non-AML regulatory obligations in a number of ways that dovetail with challenges faced in implementing compliant AML programmes.[63]

In sum, the potential application of multiple regulatory schemes and the absence of bright line tests make ascertaining the regulatory status of particular customer types and activities labour-intensive. Many FIs are accordingly taking a conservative approach and not opening such accounts, while others have proceeded on a case-by-case basis. As the following sections illustrate, the potential for different standards and consequences to attach to cryptocurrency services that cross borders further complicates these assessments.

(c) Enforcement Trends

While many of the early enforcement actions in the United States targeting cryptocurrency businesses have involved claims of fraud[64] or failure to register with appropriate regulators,[65] there have been a few examples of enforcement actions targeting VCEs for AML programme failures and there appears to be a growing focus on AML enforcement across regulators that will inevitably extend to cryptocurrency businesses.

In May 2015, FinCEN brought its first ever action against a VCE for AML programme failures when it assessed a civil money penalty against Ripple Labs Inc. and its subsidiary XRP II LLC (Ripple) for wilful violations of the BSA's registration, programme and reporting requirements.[66] Specifically, FinCEN determined that Ripple was acting as an MSB and selling its virtual currency without registering as an MSB with FinCEN, and that it had failed to implement and maintain an adequate AML programme designed to protect its products from use by money launderers or terrorist financiers.[67] Further, Ripple failed to report suspicious activity related to several suspect financial transactions in violation of its BSA SAR-filing requirements.[68] FinCEN's press release announcing the penalty cited its 2013 guidance as having clarified the applicability of regulations implementing the BSA and the requirement to register as MSBs under federal law to virtual currency exchangers and administrators.[69] Ripple ultimately agreed to pay a USD700,000 penalty in addition to forfeiting USD450,000 to settle potential federal criminal liability,[70] and agreeing to a number of remedial actions including to only engage in its virtual currency activity through a registered MSB, to conduct a three-year look-back to identify suspicious transactions, to implement and maintain an effective AML programme, and a requirement to retain external independent auditors to review their compliance with the BSA every two years.[71]

In its second supervisory enforcement action against a virtual currency exchange, FinCEN assessed a USD110,003,314 civil money penalty against Canton Business Corporation (BTC-e), then one of the world's largest virtual currency exchanges by volume, and a USD12 million civil money penalty against one of BTC-e's Russian operators for wilful violations of the BSA and its implementing regulations in July 2017.[72] BTC-e and its operator were also indicted in federal court for violations of federal criminal AML laws.[73] FinCEN determined that BTC-e lacked basic controls to prevent the use of its platform for illicit purposes, and that the virtual currency exchange actually attracted a customer based that consisted largely of criminals seeking to launder the proceeds of their crimes.[74] In its press release announcing the penalty against the foreign-located exchange, FinCEN stated that "[r]egardless of its ownership or location, the company was required to comply with U.S. AML laws and regulations as a foreign-locted MSB including AML programme, MSB registration, suspicious activity reporting, and recordkeeping requirements".[75]

Since 2017, several individuals have faced criminal charges resulting in prison sentences for illegally exchanging and or transferring virtual currency without registering with FinCEN as an MSB. A July 2018 example involved a California woman who was sentenced to a year in prison by the District Court for the Central District of California for operating a digital currency exchange without registering with FinCEN as an MSB, and for violations of the federal criminal AML laws.[76]

Beyond FinCEN and the Department of Justice, the CFTC[77] and the SEC[78] have both taken recent actions indicating that they intend to continue to focus their enforcement authority on ensuring BSA compliance at all types of covered financial institutions subject to their supervision. In September 2018, the CFTC announced the formation of a new Bank Secrecy Act Task Force within the CFTC's Division of Enforcement, to ensure that FCMs and IBs comply with their AML obligations under the BSA.[79] While BSA requirements have applied to FCMs and IBs since 2003,[80] the CFTC has traditionally only performed the role of examiner in relation to FCM and IB compliance with the BSA, with FinCEN taking the lead in enforcement.[81] However, it appears that the CFTC now views it role in relation to BSA compliance as much broader. This new focus on enforcement could be due in part by the increasing focus on cryptocurrency regulation and the particular AML risks presented by cryptocurrency businesses, combined with the fact that the CFTC has successfully argued that cryptocurrencies are commodities subject to CFTC regulation under the CEA. Increasingly, US financial services industry regulators appear to be eager to use their enforcement mechanisms to regulate domestic and foreign cryptocurrency businesses.

European Union Regulatory Approach

The final text of the most recent European-level AML directive, the Fifth Money Laundering Directive ("**MLD5**"),[82] was published in the Official Journal of the European Union on June 19, 2018 and must be implemented by EU Member States by January 10, 2020. This is the first European Union-level money laundering directive to explicitly address the regulation of cryptocurrency.[83]

MLD5 extends the definition of "obliged entities" to include virtual currency exchanges[84] and custodial wallet providers, thereby requiring such entities to comply with the same AML requirements applied to traditional financial institutions under the EU's Fourth Money Laundering Directive ("**MLD4**")[85] – including CIP and beneficial ownership identification, KYC, transaction monitoring, and suspicious activity reporting – and subjects those entities to supervision by the competent national authorities for these areas.

While MLD5 was pending, some EU jurisdictions acted to extend AML obligations to certain cryptocurrency services on their own. As shown by the following examples, there is currently significant variation, with some Member States (such as Germany and Italy) having substantially implemented an MLD5-type regime through national law or regulatory actions, and other Member States (such as the UK and the Netherlands) having thus far left cryptocurrency trading largely outside the AML regulatory regime.

(a) Italy

When Italy amended its AML Decree[86] in compliance with MLD4 in 2017 (which was done via a legislative decree, "**AML4 Decree**"),[87] it simultaneously incorporated definitions for cryptocurrency consistent with the FATF-definition[88] and classified cryptocurrency service providers[89] that provide cryptocurrency-to-fiat conversion services as "non-financial intermediaries" regulated under the AML Decree.[90] Such service providers are consequently subject to Italian AML obligations,[91] including KYC,[92] recordkeeping and communications to the authorities,[93] suspicious transaction reporting,[94] and, as a consequence of the pseudo-anonymity of blockchain users, enhanced due diligence ("**EDD**").[95] Article 8 of the AML4 Decree further requires cryptocurrency service providers to register in a special section of the Italian Registry of currency exchange professionals[96] and to communicate to the Ministry of Economy and Finance about exchange activities carried out within the Italian territory (an issue that can be particularly complex given the decentralised, global nature of cryptocurrency transactions).[97] The Ministry of Economy and Finance published a draft decree outlining these communication requirements in February 2018, but as of this writing, the decree is still under consultation.[98]

Although Italy's investment services authority, CONSOB,[99] has not yet taken a clear position in relation to transactions in cryptocurrencies, at least one Italian court has found that the sale and conversion of cryptocurrencies to legal tender could in theory constitute a form of investment services in the context of proprietary trading.[100] A 2015 Bank of Italy communication[101] on the prudential risks of cryptocurrency further suggested that some cryptocurrency functions could violate criminal provisions of Italian banking law, which reserve certain banking, payment, and investment services exclusively to authorised entities.[102] These precedents suggest the potential for collateral risk from serving unlicensed entities or, in the extreme case, handling illicit proceeds as a consequence of serving non-compliant cryptocurrency businesses in Italy. In addition to the above, it is also worth remarking that recently (19 March 2019) CONSOB launched a public consultation with the purpose to determine the legal nature and the relevant regime applicable to the issuance or exchanges of cryptoassets. The public consultation is addressed to all entities and individuals potentially interested in cryptoassets (e.g. investors; consumers; issuers of cryptoassets; and financial intermediaries) and the term to deliver opinions and comments is set on 19 May 2019.

(b) Germany

The German Federal Financial Supervisory Authority ("**BaFin**") considers cryptocurrencies that have the character of a cash instrument to be "financial instruments" under the German Banking Act ("**KWG**").[103] However, in September 2018, this administrative practice was challenged by the Berlin Court of Appeal. The court held that Bitcoin was not a "financial instrument" and would therefore not fall under the KWG. Since BaFin is not obliged to change its administrative practice after a decision reached in an individual criminal proceeding, the future application of the KWG on cryptocurrency exchanges remains uncertain. In February 2019, the BaFin noted that it maintains its former view.

As in the U.S., use of cryptocurrency as payment for goods and services and the sale or exchange of self-procured cryptocurrency would not trigger AML regulation, and such users need not seek authorisation under applicable German banking laws.[104] However, commercial dealings with cryptocurrencies can trigger an authorisation requirement where the platform involves (i) buying and selling cryptocurrency in order to carry out principal broking services, or (ii) operating as a multilateral trading facility. Providers that act as "currency exchanges" offering to exchange legal tender for the purposes of proprietary trading, contract broking, or investment broking, are also generally subject to authorisation. Finally, underwriting an ICO may be regulated underwriting or placement business within the ambit of applicable German banking laws.

When such commercial dealings with cryptocurrencies trigger an authorisation requirement, the business must obtain a licence as a credit institution or financial services institution under applicable German banking laws, and is treated as an "obliged entity"[105] under the German Money Laundering Act ("**GWG**"),[106] transposing the MLD4 AML requirements.[107] Under the still-to-be-transposed MLD5, it is envisaged that firms operating centralised cryptocurrency exchanges or custodial wallet providers for cryptocurrencies shall also fall under the GWG. However, the legislator's planned approach to implement MLD5 in Germany and the timing for this is still unclear. It is also noteworthy that BaFin has suggested that whether a cryptocurrency

is also a security must be assessed on a case-by-case basis, with the rights associated with the respective token as the decisive factor.[108] If a token is also classified as a security (beyond the classification of a mere unit of account (*Rechnungseinheit*)), this may in particular trigger conduct and prospectus requirements that go beyond licensing requirements and a resulting AML-regulation.

(c) The Netherlands

In contrast to Germany and Italy, the Netherlands has not yet formally extended their AML regulations in order to cover cryptocurrency-related services.

The 2013 conclusion of the Dutch Ministry of Finance that cryptocurrencies are neither "electronic money" nor 'financial products' within the meaning of the Dutch Financial Supervision Act ("**DFSA**")[109] has provided assurance that virtual currencies and wallet services for currency-like cryptocurrencies fall outside the scope of the DFSA.[110] Cryptocurrencies also do not (yet) qualify as "common money".[111] Consequently, issuers of cryptocurrencies, exchange-platforms and undertakings offering wallet services are in general not covered institutions for purposes of the Dutch Act for the Prevention of Money Laundering and Financing of Terrorism ("**Wwft**").[112]

However, the Dutch Central Bank (*De Nederlandsche Bank*, "**DNB**") and the Dutch Authority for the Financial Markets (*Autoriteit Financiële Markten*, "**AFM**") have provided guidance regarding the qualification of cryptocurrencies as "financial instruments" as mentioned in the DFSA. In their joint advice, the DNB and the AFM concluded that currently, under Dutch law, most cryptocurrencies do not qualify as a financial instrument under the DFSA but qualify as a prepaid right to access or use a provider's future services.[113] According to the AFM, only in certain cases cryptocurrencies qualify as a "security" and hence as a "financial instrument" under the DFSA, for example, when the holder of the cryptocurrency has a right to receive dividends from the issuer of the cryptocurrency or when the cryptocurrency resembles "traditional" securities such as bonds.[114] Investment firms facilitating the trade in or providing advice regarding such cryptocurrencies qualify as "institutions" as mentioned in the Wwft. Such investment firms must meet certain obligations under the Wwft, such as conducting client due diligence and monitoring transaction performed by clients. Due to the broad definition of "client" in the Wwft and the high risks associated with cryptocurrencies, the AFM concluded that investment firms must conduct enhanced due diligence investigations regarding client-investors, but also regarding professional counterparties selling cryptocurrencies, the issuer of the cryptocurrencies and intermediaries and platforms facilitating the trade in the cryptocurrencies.[115]

When MLD5 is implemented in Dutch law, all undertakings providing exchange services between cryptocurrencies and fiat currencies which are seated in the Netherlands or offering their services to Dutch residents will fall within the scope of the Wwft. The same applies to undertakings providing custodian wallets for cryptocurrencies. The Dutch Ministry of Finance, however, does not only wish to register such undertakings as proposed in MLD5, but has proposed that such undertakings require prior authorisation from DNB before offering their services.[116] The Dutch Ministry of Finance has proposed that these undertakings should function as gatekeepers of the (Dutch) financial system. Prior to their authorisation, DNB will assess whether these undertakings are able to fulfil their role as gatekeepers by assessing whether the undertakings are able to comply with their obligations under the Wwft and by assessing the integrity and fitness of their ultimate beneficiaries and management.[117] DNB and the AFM are supporters of this licensing regime, but the Dutch Parliament has yet to vote on this proposal.

(d) The UK

In the UK, regulators have recognised that cryptoassets vary significantly both in terms of the rights they confer on their owners, as well as their designed use. Accordingly, the UK Cryptoassets Taskforce ("the **Taskforce**"), which was established in March 2018 and comprises HM Treasury, the Bank of England and the UK Financial Conduct Authority ("**FCA**"), developed a framework[118] that categorises cryptoassets into three categories:

i. Exchange tokens – these are not issued or backed by any central authority and are intended and designed to be used as a means of exchange. Examples include Bitcoin and Litecoin.

ii. Security tokens – these have specific characteristics that mean they meet the definition of a "specified investment" for the purposes of the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 ("**RAO**") similar to, for example, a share or debt instrument.

iii. Utility tokens – these grant holders access to a current or prospective product or service but do not typically have the characteristics of "specified investments".

The FCA confirmed in its recent consultation paper entitled "Guidance on Cryptoassets" that its prevailing view is to treat exchange tokens as falling outside the regulatory perimeter[119] and that they are not expected to be "specified investments" for the purposes of the RAO. This echoes statements made by the FCA's chief executive Andrew Bailey in 2017, that virtual "commodities" like Bitcoin are not currently regulated by UK financial regulatory authorities and that it is up to Parliament to decide on any changes to those rules.[120] Conversely, the FCA confirmed that certain tokens such as security tokens (including those issued as part of an ICO) may well constitute transferable securities and fall within the prospectus regime under the Financial Services and Markets Act 2000 ("**FSMA**"), or alternatively, depending upon how they are structured, some tokens may instead amount to a collective investment scheme under section 235 of the FSMA. Derivatives that reference a cryptoasset are also capable of being regulated investments.[121]

Unless one of the regulated financial services regimes above is triggered, cryptoasset activities are unlikely to currently fall within the scope of the UK Money Laundering Regulations 2017.[122] Changes under 5MLD (supported by the UK Treasury) would result in fiat-to-crypto exchanges and custodian wallet providers' activities being brought within the scope of AML laws. Following the work of the Taskforce, the UK government also intends to consult on broadening the UK's approach to go beyond the requirements of 5MLD to include:

- exchange services between different cryptoassets, to prevent anonymous 'layering' of funds to mask their origin;
- platforms that facilitate peer-to-peer exchange of cryptoassets, which could enable anonymous transfers of funds between individuals;
- cryptoasset ATMs, which could be used anonymously to purchase cryptoassets; and
- non-custodian wallet providers that function similarly to custodian wallet providers, which may otherwise facilitate the anonymous storage and transfer of cryptoassets.

Additionally, the UK government proposes to consult on whether to require firms based outside the UK to comply with these regulations when targeting and providing services to UK consumers. The rationale is to prevent illicit actors in the UK from dealing with firms based abroad and thereby bypassing UK regulation.

As part of developing a robust AML/CTF framework for cryptoassets, the UK government has asked the FCA to consider taking on the role of supervising and overseeing firms' fulfilment of their AML/CTF obligations in relation to crypto activities. The Taskforce's

Report notes that the UK government will consult on this before confirming the identity of the supervisor. The FCA has also taken action in relation to regulated firms who, as part of their business activities, interact with cryptoassets. In June 2018, the FCA issued a letter to CEOs of all banks, setting out appropriate practice for the handling of the financial crime risks associated with cryptoassets.[123]

On an international stage, the UK has been actively engaging in discussions to ensure a coordinated global response to the financial crime risks posed by cryptoassets. The UK continues to be a leading voice in the discussions of FATF, which continues to issue and update guidance on the AML/CTF standards that apply to cryptoassets.

Separately, where firms operate within the regulatory perimeter without correct FCA authorisation (e.g., by issuing security tokens without FCA authorisation), such breaches would be a criminal offence, and thereby may give rise to a predicate crime for certain money laundering offences under the Proceeds of Crime Act 2002 ("**POCA**"). Moreover, cryptoassets or the proceeds of their sale could also be the subject of a restraint order or confiscation order to the extent that they constitute criminal property under POCA, and concealing or handling such criminal property could trigger the money laundering offences under POCA.[124] Indeed, the recent case of *R v Teresko (Sergejs)*[125] demonstrates that the UK courts had little difficulty in concluding that Bitcoin could be the subject of a seizure order pursuant to section 47A-S of POCA.

Asia-Pacific Region

Regulatory practices in Asia diverge even more than in Europe. At the extreme end, China currently prohibits commercial issuance and exchange cryptocurrency services. In contrast, Japan and Australia both now have regimes for licensing and supervising VCEs and other cryptocurrency businesses.

(a) China

China has taken perhaps the strictest approach to cryptocurrency of the world's major economies, effectively prohibiting all issuance and exchange services for cryptocurrency in the country.

Chinese regulators took a wary view beginning in December 2013, when the People's Bank of China (the "**PBOC**"), the central regulatory authority for monetary policy and financial industry regulation, issued a joint circular with other Chinese regulators emphasising the AML risk of Bitcoin and other cryptocurrencies, and requesting that all bank branches extend their money laundering supervision to institutions that provide cryptocurrency registration, trading, and other services, and urge these institutions to strengthen their monitoring of money laundering. In 2016, a PRC-incorporated VCE platform was found partially liable for AML violations due to its failure to perform KYC while offering cryptocurrency registration and trading services.[126]

Subsequently, in September 2017, the PBOC issued a joint announcement (the "**Announcement**"), affirming that cryptocurrencies do not have legal status or characteristics that make them equivalent to money, and should not be circulated and used as currencies.[127]

- On the issuance side, the Announcement banned "coin offering fundraising", defined as a process where fundraisers distribute so-called "cryptocurrencies" to investors in return for financial contributions, and classified illegal distribution of financial tokens, illegal fundraising or issuance of securities, and fraud or pyramid schemes as financial crimes in this context. Organisations and individuals that raised money through ICOs prior to the date of the Announcement were commanded to provide refunds or make other arrangements to reasonably protect the rights and interests of investors and properly handle risks.
- On the exchange side, the Announcement required cryptocurrency trading platforms to cease offering exchange of cryptocurrency for statutory (fiat) currency, acting as central counterparties for cryptocurrencies transactions, or providing pricing, information, agency or other services for cryptocurrencies.
- In a press conference in March 2018, the former president of the PBOC Zhou Xiaochuan said that the future regulation on cryptocurrency would be very dynamic depending on the development of technology and relevant tests or evaluations.[128] However, at the current stage China is still tightening its policy in order to further eliminate illegal token fundraising, taking measures to block overseas trading platforms offering cryptocurrency exchange services to PRC residents.[129]

Because of the criminalisation of unlicensed cryptocurrency issuances, capital or fees that have been acquired through a coin release in China are likely to be viewed as illicit proceeds for purposes of both Chinese and other countries' AML laws. That said, although discouraged by the PRC authorities, individual purchase or peer-to-peer trading of crypto is not banned from a PRC law perspective.

(b) Japan

In May 2016, Japan amended its Payment Services Act to provide for a definition of cryptocurrency[130] and to create a registration requirement for "Virtual Currency Exchange Operators" ("**VCEOs**").[131] VCEO licences permit holders to engage in the exchange, purchase, sale, and safekeeping of cryptocurrencies on behalf of third parties. VCEOs are designated as "Specified Business Operators" subject to national AML rules contained in the Act on the Prevention of Transfer of Criminal Proceeds, including CIP and suspicious transaction reporting.[132] Since licences were first issued to VCEOs on September 29, 2017, the FSA, which exercises regulatory authority over Banks and other financial institutions via delegated authority from the Prime Minister, has begun conducting on-site inspections of VCEOs and has forced at least one exchange to cease operations until it remedies compliance deficiencies, including its AML compliance. The prospect of enforcement of AML regulations appears to have caused some companies to withdraw their applications to become VCEOs in recent months.[133]

(c) Australia

In Australia, cryptocurrency is regulated both as a currency and as a financial instrument such as a share in a company or a derivative depending on the features of the coin.[134] Businesses that support cryptocurrency-to-fiat exchange are classified as "digital currency exchanges" and are required to comply with the AML laws and regulations under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006; however, the law was changed in 2017 to exclude most ICOs from such requirements.[135] For entities that are subject to the law, the Australian Transaction Reports and Analysis Centre ("**AUSTRAC**") has published a compliance guide for providing guidance on how to implement an AML-CTF compliance programme.[136]

Cryptocurrency Risk Considerations

Elevated AML Risks in Cryptocurrency

Cryptocurrency markets are potentially vulnerable to a wide range of criminal activity and financial crimes. Many of these risks materialise not on the blockchain itself, but in the surrounding ecosystem of issuers, VCEs, and wallets that support consumer access to DLT. Rapidly evolving technology and the ease of new cryptocurrency creation are likely to continue to make it difficult for law enforcement and FI's subject to AML requirements to stay abreast of new criminal uses.

1. **Trafficking in Illicit Goods**: Cryptocurrencies provide an ideal means of payment for illegal goods and services, from narcotics, human trafficking, organs, child pornography, and other offerings of the "dark web". The most notable of these was the online contraband market Silk Road, in which all transactions between the buyers and sellers were conducted via Bitcoin. The site was eventually shut down by the U.S. Federal Bureau of Investigation and the founder was convicted of seven counts of money laundering, drug distribution, conspiracy, and running a continuing criminal enterprise.[137]
2. **Hacking and Identity Theft**: Crypto wallets and VCEs provide hackers with attractive targets for financial fraud and identity theft. If an account is hacked via one of these services, crypto holdings can be easily exfiltrated to anonymous accounts and liquidated for fiat or other assets, with little or no possibility of reversing or cancelling the transactions after detection.
3. **Market Manipulation and Fraud**: While the blockchain in principle allows all actors to view and monitor exchange transactions, the ability to detect and deter insider trading, front-running, pump-and-dump schemes, and other forms of market abuse involving unregistered ICOs and unlicensed VCEs is severely limited. The absence of regulatory oversight with respect to unregistered offerings and the ease with which criminal actors can create new accounts to execute manipulative schemes makes these markets vulnerable.
4. **Facilitating Unlicensed Businesses**: Variations in the legal and regulatory requirements surrounding cryptocurrency services in different jurisdictions create added challenges in determining whether cryptocurrency businesses are in compliance with local rules. Providing financial services to non-compliant entities could, in some circumstances, implicate illicit proceeds provisions.

In addition, the anonymity, liquidity, and borderless nature of cryptocurrencies makes them highly attractive to potential money launderers.

5. **Placement**: The ability to rapidly and anonymously open anonymous accounts provides a low-risk means for criminal groups to convert and consolidate illicit cash.
6. **Layering**: Cryptocurrency provides an ideal means to transit illicit proceeds across borders. For example, the U.S. Drug Enforcement Administration's 2017 National Drug Threat Assessment identified cryptocurrency payment as an "[e]merging ... vulnerability" in trade-based money laundering, in which cryptocurrency is used to transfer funds across borders in "repayment" for an actual or fictitious sale of goods. The DEA particularly identified Chinese demand for Bitcoin, helpful to avoid Chinese capital controls, creating a market for bulk fiat cash from the U.S., Europe, and Australia, with a mix of licensed and unlicensed over-the-counter Bitcoin exchanges serving as the go between.[138] Similarly, in April 2018, European authorities busted a money laundering operation that used Bitcoin purchased from a Finnish exchange to transfer cash proceeds of drug trafficking from Spain to Colombia and Panama.[139] Unregistered ICOs also provide opportunities for large scale layering. If the money launderers also control the ICO, then they can use a fraudulent "capital raising" to convert their crypto-denominated illicit proceeds back into fiat currency.
7. **Integration**: The growing list of goods accepted for purchase with cryptocurrencies expands integration opportunities. For example, the Italian National Council of Notaries recently advised notaries to make a suspicious transaction report every time they have to assist parties in the purchase of real estate by means of cryptocurrencies, since the anonymity of the crypto-payment's source would prevent the identification of the parties of the transaction.[140] The willingness of ICOs to trade crypto-for-crypto could also lead to criminal enterprises taking large stakes in crypto businesses, with or without the awareness of those businesses.
8. **Terrorism Financing and Sanctions Evasion**: The same anonymity and ease of creation makes crypto-accounts ideal for persons to receive payments that might otherwise trigger terrorism financing or sanctions red flags. Although the use of cryptocurrencies is not yet widespread in terrorism financing, terrorist groups have been experimenting with cryptocurrencies since 2014 and Bitcoin has been raised for such groups through social media fundraising campaigns.[141] States targeted by sanctions have also taken an interest in creating their own state-sponsored cryptocurrency, with Venezuela debuting such a coin in February 2018.[142]

All of these risks are heightened among the unregulated sectors of the cryptocurrency markets. Given regulatory pressure to reject anonymity and introduce AML controls wherever cryptocurrency markets interface with the traditional financial services sector, there are signs that the cryptocurrency market is diverging, with some new coins being created to be more compatible with existing regulations while "privacy coins" prioritise secrecy of transactions and identities in order to facilitate off-market transactions.[143]

Managing Risk of Cryptocurrency Users and Counterparties

In view of the issues discussed above, financial institutions should approach services and customers connected to cryptocurrency with a full understanding of their respective roles with cryptocurrencies and any potential elevated risks. As with any new line of business, then, the central AML compliance question for financial institutions will be whether they can reasonably manage that risk. FIs that choose to serve new lines of business or customer types should perform a risk assessment so that they can tailor policies and procedures to ensure that AML obligations can still be fulfilled in the cryptocurrency context.

(a) Fulfilling Identification and Monitoring Requirements in the Cryptocurrency Context

The ability to confirm the identity, jurisdiction, and purpose of each customer is essential to the fulfillment of AML programmes. In spite of the inherent challenges that cryptocurrencies pose in all these dimensions, an FI must ensure that its policies and procedures allow it to perform these core functions with the same degree of confidence in the cryptocurrency context as they do for traditional services. While the precise measures necessary will inevitably depend on the particular customer and service, some broad points can be made.

- **Customer and Counterparty Identification**: Although the pseudo-anonymity of holders is central to many cryptocurrencies, an FI cannot enter into a customer relationship unless it has confirmed the true identity of the customer. Assuming that CIP has been performed on the customer with respect to other financial services, this is most likely to arise in the context of establishing proof of ownership over crypto-assets held by the customer outside of the FI. Similarly, although U.S. AML rules do not require FIs to perform CIP on transaction counterparties, acquisition of baseline counterparty information will typically be necessary in order to provide a reasonable assurance of sanctions compliance, as well as supporting anti-fraud and transaction monitoring efforts. In the cryptocurrency context, appropriate procedures might resemble those used to confirm ownership of non-deposit assets, such as chattel property or, even better, digital assets such as internet domains. At a minimum, the information obtained about the parties to cryptocurrency-related transactions would likely need to be sufficient to allow the FI to apply the sanctions list screening procedures it applies to other transactions of comparable risk. Since procedures should be risk-based, FIs may find it appropriate to apply more

enhanced measures to the verification of crypto-holder assets in view of the underlying risks posed by such assets.

- **Diligence/KYC, Account Monitoring, and Suspicious Activity**: The obligation to develop a reasonable understanding of "the purpose and intended nature of the business relationship"[144] generally would apply equally when that relationship involves dealings in cryptocurrency. Again, given the special concerns surrounding cryptocurrency markets, FIs may determine that heightened due diligence is appropriate in this context. Similarly, FIs may find it appropriate to develop special red flags that apply to dealings in cryptocurrency markets, and to train responsible employees accordingly.
- **Transaction Reporting and Recordkeeping**: Where covered transactions involving cryptocurrency surpass specified thresholds, FIs will need to record or report the same information as would apply for a non-cryptocurrency transaction. As with updates to CIP, the policies and procedures in place should give the FI assurance that the information that it obtains for this purpose is accurate and is sufficient for auditing review. Importantly, true identification of the holders of cryptocurrency accounts from which funds are sent and received will enable the FI to appropriately apply transaction monitoring controls, including aggregation requirements[145] and detection of structuring payments.[146] To the extent that the FI intends to rely on data analytics for these functions, such systems should be in place and tested before the FI begins processing such transactions.

(b) Assessing and Managing Risks of Customers Dealing in Cryptocurrency

Special AML considerations arise when the customer of an FI is itself a cryptocurrency business. VCE or wallet services potentially will themselves typically be classified as AML-obligated entities, depending on the jurisdiction(s) in which they offer services. A currency administrator, such as the issuer of an ICO, may also be subject to AML obligations, and all three business types may be subject to other financial services licensing or registration regimes. We outline some of these issues below.

(i) Crypto-Business Customers that Are Financial Institutions

FIs may be required to conduct additional diligence when onboarding and monitoring crypto-business customers that are themselves FIs.

In the U.S., FinCEN guidance on servicing MSB accounts drafted prior to the advent of cryptocurrency remains applicable to accounts for VCEs and wallets that are MSBs.[147] In addition to performing CIP, this guidance requires FIs to: confirm FinCEN registration status of the MSB (or application of an exemption); confirm compliance with state and local licensing requirements, if applicable; confirm agent status, if applicable; and conduct a basic BSA/AML risk assessment to determine the level of risk associated with the account and whether further due diligence is necessary.[148] While an FI generally is not responsible for the effectiveness of its customers' AML programmes, deficiencies in this area can be a clear red flag when evaluating a customer's particular risk level.[149] In particular, FinCEN advises that "due diligence [of NBFI customers] should be commensurate with the level of risk...identified through its risk assessment", such that if an NBFI presents "a heightened risk of money laundering or terrorist financing, [the FI] will be expected to conduct further due diligence in a manner commensurate with the heightened risk".[150]

Onboarding and risk assessment for a cryptocurrency business is likely to encompass a number of questions related to the business' compliance with applicable regulatory requirements:

1. **Information Gathering**: Does the customer's business and compliance model permit them to collect information sufficient to perform CIP and to risk rate its own customers? To obtain information as to counterparties and the locations of transactions?
2. **Monitoring and Reporting**: Does the customer have mechanisms in place for account monitoring and procedures in place for required reporting?
3. **Geographic Controls**: Is the service able to control the jurisdictions in which its services are accessed?
4. **Legal Status and Licensing and Registration Compliance**: Has the service assessed the legality of its services in all the jurisdictions in which it operates? Has it undertaken the required licensing and registration outside the U.S.?

In some cases, cryptocurrency businesses may argue that, for legal or technical reasons, their services are not covered by the existing FinCEN registration guidance or by any state regime, and that they are therefore not required to register. These arguments may have merit in individual cases, but FIs may need to take some steps to reach their own opinion as to the validity of these assessments (particularly in cases where there is some question as to the legality of the enterprise), and may be advised to factor registration risk into their overall assessments of whether and how to provide services to the customer.[151]

(ii) Other Crypto-Business Risks

Even where an FI has assurance that the customer crypto-business is not an AML regulated entity, the FI should update policies and procedures in order to be able to account for heightened money laundering risk posed by the business.

The question of geographic control also warrants special attention in the context of servicing crypto-businesses. In addition to the risk of dealing with sanctioned persons and jurisdictions, the current absence of uniformity in the treatment of cryptocurrency activities – in particular, the differing registration requirements and the prohibition on issuance and exchange services in China – creates legal risk similar to that of online gambling or other services that are legal in some jurisdictions, but not others. The inability to control where services are offered raises the possibility that the enterprise itself is engaging in prohibited conduct. Where such prohibition is criminal, these violations could cause the crypto-business's earnings to be classified as illicit proceeds for the purposes of criminal AML provisions.[152] Regardless of whether national law applies, a strict liability approach or a knowledge/recklessness requirement to such acceptance, financial institutions' compliance programmes must include reasonable measures to detect and prevent such facilitation. Even where there is no risk of criminal violation, the FI providing services to a crypto-business should consider whether it would provide the services to a non-crypto-business whose registration status was in doubt.

Even for ICOs that do not qualify as obligated entities under relevant AML rules, FIs should carefully evaluate whether the structure of the ICO presents AML risk. An ICO should receive particular scrutiny if (i) the token sale is not capped per user, such that unlimited amounts of funds can be transferred to the ICO issuer, and (ii) the ICO intends to convert a portion of the raised funds to fiat. FIs should examine terms and conditions of an issuance to determine whether the issuer has controls in place to avoid wrongdoing.

Acknowledgment

The authors wish to thank the following attorneys for their significant contributions to this chapter: Jason Denisenko (Australia); Jane Jiang, Tiantian Wang, Jason Song, and Aubrey Tang (China); Alexander Behrens, Janis Petrowsky, David Schmid and Gero Pogrzeba (Germany); Giovanni Battista Donato, Emanuela Semino, Luca Di Lorenzi, and Amilcare Sada (Italy); Tokutaka Ito (Japan); Abas Hoesseinzada and Daphne van der Houwen (the Netherlands); Ben Regnard-Weinrabe and Heenal Vasu (UK); and Bill Satchell and Justin Cooke (U.S.).

Endnotes

1. As defined by the Financial Asset Task Force ("**FATF**"), the term "cryptocurrency" refers to any "math-based, decentralised convertible virtual currency that...incorporates principles of cryptography to implement a distributed, decentralised, secure information economy", FATF, *Virtual Currencies Key Definitions and Potential AML/CFT Risks* (June 27, 2015), http://www.fatf-gafi.org/media/fatf/doc uments/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (hereinafter "FATF 2015 Guidance"). The first cryptocurrency to come into existence is called Bitcoin, and other cryptocurrencies have since been created adopting parallel principles. Cryptocurrencies may overlap to an extent with products created via so-called "initial coin offerings" or "ICOs" which are discussed further in Part 2, *infra*.
2. Nakamoto, Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System* (May 24, 2009), https://bitcoin.org/bitcoin.pdf.
3. Valuations according to Cryptocurrency Market Capitalizations, https://coinmarketcap.com (last visited Apr. 4, 2018, 10:00 EST).
4. Many cryptocurrencies use a process known as "mining" to produce new crypto-coins or other cryptocurrency units. This process often involves extensive mathematical calculations, and may require significant energy and computing resources.
5. For the purpose of this article, the term "FIs" encompasses any class of persons that is obligated to undertake AML measures under the law or regulation of a particular jurisdiction. Different terms of art may be used in different jurisdictions (e.g., "financial institution", "obligated person", etc.).
6. A process through which consensus with respect to digital data replicated, shared, and synchronised across multiple nodes (or ledgers) affords confidence as to the authentication and accuracy of the shared digital data. A distinguishing feature is that there is no central administrator or centralised data storage responsible for maintaining or authenticating the accuracy of data.
7. FATF 2015 Guidance, *supra* note 2, at 26.
8. "Convertibility" means that the cryptocurrency "has an equivalent value in real currency and can be exchanged back-and-forth for real currency". As a definitional matter, FATF focuses on *de facto* convertibility – i.e., existence of a market for exchange – rather than "*ex officio* convertibility" or convertibility "guaranteed by law". FATF 2015 Guidance, *supra* note 2, at 26–27.
9. A "non-convertible" cryptocurrency is specific to a particular virtual domain or online community and does not necessarily have an established value in terms of a fiat currency. *Id*. at 7.
10. Defined by FATF as "hav[ing] a single administrating authority (administrator) – i.e., a third party that controls the system. An administrator: issues the currency; establishes the rules for its use; maintains a central payment ledger; and has authority to redeem the currency (withdraw it from circulation)". *Id.* at 27.
11. Defined by FATF as "distributed, open-source, math-based peer-to-peer virtual currencies that have no central administrating authority, and no central monitoring or oversight". Examples include Bitcoin, LiteCoin, and Ripple. *Id.* at 27.
12. *See*, *e.g.*, Gavin Wood, *Ethereum: A Secure Decentralised Generalised Transaction Ledger* (Apr. 2014), http://gavwood.com/paper.pdf (unpublished manuscript).
13. Jay Clayton, Chairman, SEC, Statement on Cryptocurrencies and Initial Coin Offerings (Dec. 11, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11.
14. *See, e.g.,* Jacob Kleinman, *How Does Blockchain Work?* (Jan. 16, 2018), https://lifehacker.com/what-is-blockchain-1822094625; Ameer Rosic, *What is Blockchain Technology? A Step-by-Step Guide For Beginners*, Blockgeeks (2016) https://blockgeeks.com/guides/what-is-blockchain-technology/; Marco Iansiti & Karim R. Lakhani, *The Truth About Blockchain*, Harvard Bus. Rev. (Jan./Feb. 2017), https://enterprisersproject.com/sites/default/files/the_truth_about_blockchain.pdf.
15. *See generally* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Bitcoin Project, http://bitcoin.org/bitcoin.pdf [https://perma.cc/GXZ8-6SDR].
16. Adam Ludwin, *How Anonymous is Bitcoin?*, Coin Center (Jan. 20, 2015), https://coincenter.org/entry/how-anonymous-is-bitcoin.
17. *See*, *e.g.*, J. Luu & E.J. Imwinkelried, *The Challenge of Bitcoin Pseudo-Anonymity to Computer Forensics*, Criminal Law Bulletin (2016).
18. In addition to IP address concealment, users may employ so-called "mixers" or "tumblers" to exchange their Bitcoins for another set of the same value (minus a processing fee) with different addresses and transaction histories. *See* FATF 2015 Guidance, *supra* note 2, at 28.
19. FATF 2015 Guidance, *supra* note 2, at 29.
20. Examples include CoinBase and Binance.
21. For example, decentralised trading services have emerged that facilitate counterparty price communication, rather than acting as centralised market-makers, and that may facilitate brokered trades or direct peer-to-peer price trading on this basis. Examples include Herdius, AirSwap, Raiden, and Etherdelta. *See*, *e.g.*, Balazs Deme, *Decentralized vs. Centralized Exchanges*, Medium (Jan. 24, 2018), https://medium.com/herdius/decentralized-vs-centralized-exchanges-bdcda191f767.
22. *See*, *e.g.*, Steven Mnuchin, Sec'y, U.S. Dep't of Treasury, Panel Discussion at the World Economic Forum: The Remaking of Global Finance (Jan. 25, 2018) (stating that his primary goal is "to make sure that [digital currencies are] not used for illicit activities" and, to do this, he has suggested "the world have the same regulations"); Emmanuel Macron, President of France, Special Address at the World Economic Forum (Jan. 24, 2018) (calling for "a global contract for global investment").
23. FATF, *Public Statement – Mitigating Risks from Virtual Assets* (Feb. 22, 2019), http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html.
24. Bank Secrecy Act of 1970, as amended by the USA PATRIOT Act, 31 U.S.C. §§ 5311 *et seq*.
25. *See* 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 1010.100.
26. 31 C.F.R. § 1010.100(ff).
27. 15 U.S.C. §§ 78c(a)(4)-(a)(5).
28. 7 U.S.C. § 1a(31).
29. 23 NYCRR Part 200.
30. 31 C.F.R. § 1010.100(m).
31. The term "money services business" includes any person doing business, whether or not on a regular basis or as an organised business concern, in one or more of the following capacities: (1) currency dealer or exchanger; (2) check casher; (3) issuer of travellers' cheques, money orders, or stored value; (4) seller or redeemer of travellers' cheques, money orders or stored value; (5) money transmitter; or (6) U.S. Postal Service. Excluded from this definition are banks, foreign banks, certain SEC- and CFTC-registered persons and their non-U.S. equivalents, and persons who engage in covered activities "on an infrequent basis and not for gain or profit". 31 C.F.R. § 1010.100(ff).
32. U.S. Dep't of the Treasury Fin. Crimes Enf't Network, *FIN-2013-G001 Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (Mar. 18, 2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf [hereinafter *FinCEN Guidance*]. Similar to the FATF definition, FinCEN defined "virtual currency" as a

medium of exchange that operates like a currency in some environments, but lacks attributes of real currency, such as legal tender status. FinCEN further defined "convertible virtual currency" as any virtual currency that "either has an equivalent value in real currency, or acts as a substitute for real currency". *See FinCEN Guidance* at 1–2.

33. *Id.*
34. In parallel with the FATF definitions, FinCEN defines an administrator as a business "engaged...in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency". *Id.* FinCEN defines an exchanger as a business "engaged in the exchange of virtual currency for real currency, funds, or other virtual currency". *Guidance*, *supra* note 33, at 2.
35. FinCEN's regulations provide that whether a person is a money transmitter depends on facts and circumstances. The regulations identify six circumstances in which a person is not a money transmitter, despite otherwise meeting such requirements. 31 C.F.R. § 1010.100(ff)(5)(ii)(A)–(F). As discussed below, these exemptions include instances when the entity is a registered broker or deal of commodities or securities.
36. *FinCEN Guidance*, *supra* note 33, at 3.
37. *See*, *e.g.*, Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform, FIN-2014-R011 (Oct. 27, 2014); Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System, FIN-2014-R012 (Oct. 27, 2014); Application of Money Services Business Regulations to the Rental of Computer Systems for Mining Virtual Currency, FIN-2014-R007 (Apr. 29, 2014); Application of FinCEN's Regulations to Virtual Currency Software Development; and Certain Investment Activity, FIN-2014-R002 (Jan. 30, 2014).
38. For a discussion of these categories, *see* Peter van Valkenburgh, *The Bank Secrecy Act, Cryptocurrencies, and New Tokens: What is Known and What Remains Ambiguous*, Coin Center 8 (May 20, 2017), https://coincenter.org/entry/aml-kyc-tokens. Legislation has also been proposed that would potentially extend the MSB definition to include digital wallets and cryptocurrency tumblers that merely "accept" cryptocurrency; however, the prospects of such a change are uncertain. See Senate Bill S. 1241, titled "Combating Money Laundering, Terrorist Financing and Counterfeiting Act of 2017".
39. *See* Securities Act of 1933 § 2(a)(1), 15 U.S.C. § 77b(a)(1). "The term 'security' means any note, stock, treasury stock… bond, debenture…investment contract…or, in general, any interest or instrument commonly known as a 'security'....".
40. *See, e.g.*, Jay Clayton, Chairman, SEC, *Testimony Before the Sen. Comm. on Banking, Housing, and Urban Affairs on Virtual Currencies: The Oversight Role of the U.S. Securities and Exchange Commission and the U.S. Commodity Futures Trading Commission*, 115th Cong. (Feb. 6, 2018); Jay Clayton, Chairman, SEC, Statement on Cryptocurrencies and Initial Coin Offerings (Dec. 11, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11.
41. *See, e.g.*, *In re Munchee Inc.*, Admin. Proc. File No. 3-18304, Securities Act Release No. 10445 (Dec. 11, 2017); SEC, Release No. 81207, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO* (July 25, 2017) ("DAO Report").
42. *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946).
43. *E.g.*, DAO Report, *supra* note 42, at 13–16.
44. 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).
45. *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 42. 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.
46. *E.g.*, the requirement to file a registration statement that describes the cryptocurrency issuer's business operations and management, discloses potential risks of investing in the cryptocurrency, and includes recent audited financial statements for the issuer. *See* Regulation S-K, 17 C.F.R. pt. 229; Regulation S-X, 17 C.F.R. pt. 210.
47. *E.g.*, exemptions that require investors to meet certain criteria as to financial sophistication and net worth. *See, e.g.*, 17 C.F.R. §§ 230.144A, 230.500–508.
48. 15 U.S.C. § 78c(a)(5).
49. *See* 31 C.F.R. § 1010.100(t)(2) (defining a broker or dealer in securities as a "financial institution").
50. 15 U.S.C. § 78c(a)(4).
51. *See id.* §§ 78c(a)(5), 78o(b). Note that the SEC has found that certain virtual currency exchanges meet the definition of a securities exchange under the Exchange Act. *See id.* § 78c(a)(1); 17 C.F.R. § 240.3b-16(a). The SEC also applied this view in the DAO investigation, finding that the VCEs in question were exchanges because they provided users with an electronic system that matched orders from multiple parties to buy and sell DAO tokens for execution on the basis of non-discretionary methods. DAO Report, *supra* note 42, at 17. However, because a "securities exchange" is not a "financial institution" for Bank Secrecy Act purposes, no additional AML obligations attach to this determination (and, as a practical matter, such exchanges are likely to be captured by the MSB rules).
52. *See* U.S. Commodity Futures Trading Comm'n, *Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets* (Jan. 4, 2018), https://www.cftc.gov/sites/default/files/idc/groups/public/%40customerprotection/documents/file/backgrounder_virtualcurrency01.pdf.
53. *See Commodity Futures Trading Comm'n v. McDonnell*, 18-cv-00361-JBW-RLM (E.D.N.Y. Mar. 6, 2018), https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoindroporder030618.pdf.
54. 7 U.S.C. § 1a(28).
55. 7 U.S.C. § 1a(31).
56. *See* generally 17 C.F.R. § 42.2 and 31 C.F.R. § 1026. If an entity is engaged in: (i) soliciting or accepting customer orders for the purchase or sale of commodity-based derivatives (including cryptocurrency derivatives); and (ii) accepting customer funds, securities, or property to margin, guarantee, or secure any trades or contracts that may result from such orders, that entity qualifies as a futures commission merchant (FCM) and thus as a "financial institution" under the BSA. 31 C.F.R. § 1010.100(t)(8, 9). The BSA and related regulations require FCMs and introducing brokers to establish AML programmes, report suspicious activity, verify the identity of customers and apply enhanced due diligence to certain types of accounts involving foreign persons. The CFTC has noted that, in the future, it is possible that commodity pool operators, commodity trading advisors, swap dealers, and other CFTC registrants may be required to comply with anti-money laundering regulations; however, they are not subject to such provisions at this time.
57. 31 C.F.R. §§ 1022, 1023.

58. 31 C.F.R. § 1022.380.
59. *E.g.*, a required SAR filing threshold of USD2,000 applies to transactions by, at, or through an MSB, as opposed to USD5,000 for a broker-dealer in securities. *See* 31 C.F.R. § 1023.320; *see also* Internal Revenue Serv., *Money Services Business (MSB) Information Center*, IRS.gov, https://www.irs.gov/businesses/small-businesses-self-employed/money-services-business-msb-information-center (last visited Apr. 4, 2018).
60. 31 C.F.R. § 1010.410(e).
61. 31 C.F.R. § 1010.311.
62. 31 C.F.R. § 1010.100(ff)(8)(ii).
63. For example, difficulties in identifying and verifying customers and counterparties in the DLT context could pose challenges to the maintenance of adequate books and records. Similarly, because the funds and assets of a broker-dealer's customers must be held by a qualified custodian such as a bank or the broker-dealer itself, it may be necessary to assess whether connected wallet services meet this standard. *See* 17 C.F.R. §§ 240.15c3-3, 240.17a-3.
64. *See CFTC v. Gelfman Blueprint, Inc et al*, No. 1:17-cv-07181 (S.D.N.Y. Sept. 21, 2017) (CFTC charged Gelfman Blueprint, Inc and its CEO in the first anti-fraud enforcement action involving Bitcoin filed by the CFTC); *see also CFTC v. Dean, et al*, No. 2:18-cv-00345 (E.D.N.Y. Jan. 18, 2018) (CFTC charged a Commodity Pool Operator and its Principal for engaging in a fraudulent scheme to solicit Bitcoin from investors to be pooled and invested in various commodity interests); *see also CFTC v. McDonnell, et al*, No. 1:18-cv-00361-JBW-RLM, slip op. (E.D.N.Y Mar. 6, 2018) (court held that virtual currencies are commodities under the CEA and are therefore subject to the CFTC's anti-fraud enforcement authority); *see also SEC v. PlexCorps, et al*, No. 1:7-cv-07007-DLI-RML (E.D.N.Y. Dec. 1, 2017) (SEC charged a Canadian company with fraudulently marketing tokens in an initial coin offering to US investors).
65. *See In the Matter of: BXXNA Inc d/b/a Bitfinex*, CFTC No. 16–19 (Jun. 2, 2016) (CFTC settlement order concluding that Bitfinex was operating illegally by not complying with the requirement to register as a DCM); *see also In the Matter of Munchee Inc*, Release No. 10445, Admin. File No. 3-18304 (Dec. 11, 2017) (SEC administrative proceeding brought against a California based iPhone application developer for making an illegal, unregistered securities offering in the form of an ICO); *see also SEC v. Montroll, et al.*, 1:18-cv-01582 (S.D.N.Y. Feb. 21, 2018) (SEC brought charges against an unregistered bitcoin-denominated securities and its operator for both failure to register with the SEC and also defrauding users of the exchange by misappropriating their funds).
66. *See* news release, FinCEN, 'FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger' (May 5, 2015) https://www.fincen.gov/news/news-releases/fincen-fines-ripple-labs-inc-first-civil-enforcement-action-against-virtual (Ripple concurrently entered into a settlement agreement with the United States Attorney for the Northern District of California to resolve a criminal investigation into violations of federal law for the same underlying conduct).
67. *Id*.
68. *Id*.
69. *Id*.
70. Settlement Agreement, U.S. Dep't of Justice, U.S. Attorney, Northern Dist. of Ca (May 4, 2015) https://www.justice.gov/file/421626/download.
71. *See* endnote 66.
72. *See* news release, FinCEN 'FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drug Sales' (Jul. 26, 2017), https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware.
73. FinCEN, Assessment of Civil Money Penalty No. 2017-03 (Jul. 26, 2017).
74. *Id*.
75. *See* endnote 72.
76. *See* news release, Dept. of Justice, U.S. Attny's Office Central District of CA, 'Bitcoin Maven Sentenced to One Year In Federal Prison on Bitcoin Money Laundering Case" (Jul. 9, 2018).
77. The CFTC filed a complaint against 1Pool Ltd., an international trading platform, in September 2019 for engaging in unlawful retail commodity transactions (margined in Bitcoin), failing to implement procedures to prevent money-laundering, and failing to register with the CFTC.
78. The SEC issued a cease and desist order against a U.S. broker-dealer for failure to file SARs appropriately and failure to accurately document procedures set forth in its customer identification programme. The cease and desist order was issued concurrently with the announcement that the U.S. Attorney for the Southern District of New York was bringing the first ever criminal charges against a broker-dealer for violations of the BSA in connection with the same activity.
79. *See* CFTC Release No. 7809-18 (Sept. 27, 2018).
80. In 2003 the CFTC and FinCEN jointly adopted rules implementing the Patriot Act of 2001.
81. CFTC Rule 42.2 implements the authority FinCEN delegated to the CFTC to examine FCMs and IBs and ensure that they comply with the Bank Secrecy Act regulations to which they are subject, and specifically requires every FCM and IB to comply with the applicable provisions of the Bank Secrecy Act, the FinCEN regulations promulgated thereunder, and with the requirements of 31 U.S.C. 5318(l) and 31 CFR 1026.220, which require that a customer identification programme be adopted as part of the firm's Bank Secrecy Act compliance programme. Importantly, the FinCEN rule that delegates authority to the CFTC, 31 CFR § 1010.810, provides, "[o]verall authority for enforcement and compliance, including coordination and direction of procedures and activities of all other agencies exercising delegated authority under this chapter [i.e., 31 CFR Chapter X], is delegated to the Director, FinCEN" (emphasis added). The rule only delegates to the CFTC (and other financial regulators) the authority to "examine institutions to determine compliance with the requirements of" the Bank Secrecy Act.
82. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [hereinafter EU Directive 2018/843].
83. Previously, the most recent European-level AML directive, the Fourth Money Laundering Directive ("**MLD4**"), did not explicitly address cryptocurrency, and the European Commission did not interpret its then existing regulatory guidance to require extension of the MLD4 regime to cryptocurrencies. Specifically, the European Parliament and the Council of the European Union determined that the rules and regulation of the MLD4 did not apply to "providers of exchange services between virtual currencies and fiat currencies [or to] custodian wallet providers for virtual currencies". *See* Proposal for a Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing and Amending Directive 2009/101/EC, COM(2016) 450 final (Oct. 28, 2016) [hereinafter Proposal for a Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849].
84. MLD5 defines "virtual currencies" as a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally

established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored, and traded electronically". EU Directive 2018/843, *supra* note 82.

85. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, Amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and Repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, 2015 O.J. (L 141) 73 [hereinafter EU Directive 2015/849].
86. Legislative Decree n. 231/2007 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing (21 Nov. 2007) (It.).
87. Legislative Decree n. 90/2017 (EU MLD4) (25 May 2017) (entry into force of the new AML Decree on 4 July 2017) [hereinafter AML4 Decree] (It.).
88. Defined as "a digital representation of value, not issued by a central bank or a public authority, not necessarily linked to a currency having legal tender, used as mean of exchange for the purchase of goods and services and transferred, archived and negotiated electronically" *Id.* art. 1 ¶ 2(qq).
89. Defined as "the natural or judicial person that supplies to third parties, as a professional activity, services functional to the use, exchange, storage of crypto-currencies and to their conversion from or to currencies having legal tender" *Id.* art. 1 ¶ 2(ff).
90. *Id.* art. 3 ¶ 5(i).
91. *Id.* art. 3.
92. *Id.* arts 17–30.
93. *Id.* arts 31–34.
94. *Id.* arts 35–41.
95. Because the AML4 Decree lists anonymity as one of the factors that justify performance of enhanced KYC, cryptocurrency service providers are likely be required to implement some form of EDD when servicing pseudo-anonymous cryptocurrency accounts.
96. Held by the Italian Organization of Agents and Mediators.
97. AML4 Decree, *supra* note 73, at art. 8 (by amending Legislative Decree n.141 of 13 Aug. 2010 art. 17-*bis*.).
98. Draft of Ministry on Economy and Finance Decree on Providers of Services Relating to the Use of Crypto-Currencies, (Feb. 2, 2018), http://www.dt.tesoro.it/export/sites/sitodt/modules/documenti_it/regolamentazione_bancaria_finanziaria/consultazioni_pubbliche/31.01.18_bozza_DM_prestatori_val_virtuale_.pdf (It.).
99. *Commissione Nazionale per le Società e la Borsa.*
100. Legislative Decree n. 58 of 24 Feb. 1998, art. 1 ¶ 5(a) (the "Italian Financial Law") (It.). Also, note that in some cases CONSOB prohibited the activity of intermediaries offering portfolio investments in cryptocurrencies as they did not comply with formal requirements (i.e., drafting of a prospectus subject to CONSOB's approval) provided by Italian laws and regulations for the offering of financial products to the public.
101. *Banca D'Italia Eurosistem, Avvertenza sull'utilizzo delle cosiddette "valute virtuali*", 30 Jan. 2015 (It.).
102. See Legislative Decree n. 385 of 1 Sept. 1993 arts 130–131, 131-*ter*, 166 (It.).
103. Specifically, such coins are deemed to be "units of account" (*Rechnungseinheiten*). *Gesetz über das Kreditwesen* [*Kreditwesengestz*, KWG] [Banking Act], Sept. 9, 1998 at Pt. I, Div. I(1)(11). In this sense, they are distinct from legal tender and, for decentralised cryptocurrency without entitlements toward the original issuer, are not characterised as "e-money" regulated under the Payment Services Supervision Act. *Zahlungsdiensteaufsichtsgesetz* [ZAG] [Payment Services Supervision Act], Jan. 13, 2018; BaFin article about "virtual currency": https://www.bafin.de/EN/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node_en.html (*Ger.*).
104. Likewise, the creation of new cryptocurrency by solving complex mathematical computational tasks (mining) does not constitute a regulated activity according to the KWG.
105. "*Verpflichtete*".
106. *Geldwäschegesetz* [GwG] [Money Laundering Act], Aug. 13, 2008 at §§ 2(1)(1)–(2) (*Ger.*).
107. *Inter alia*, the GWG requires obliged entities to have effective risk management systems and fulfil general due diligence requirements as defined in section 10 of GWG, including customer identification, beneficial ownership identification, and risk-based diligence and account monitoring, as well as suspicious transaction reporting regardless of the value of the asset concerned or the transaction amount under section 43 of GWG. *Geldwäschegesetz* [GwG] [Money Laundering Act], *Aug. 13, 2008, §§ 10, 43 (Ger.).*
108. Fed. Fin. Supervisory Auth., *Initial Coin Offerings: Advisory Letter on the Classification of Tokens as Financial Instruments* (Mar. 28, 2018), https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2018/fa_bj_1803_ICOs_en.html (*Ger.*).
109. *Wet op het financieel toezicht*, Art. 1:1 (Dutch).
110. *Beantwoording schriftelijke Kamervragen Nijboer over het gebruik van en toezicht op nieuwe digitale betaalmiddelen zoals de Bitcoin*, FM/2013/1939 U (19 Dec. 2013).
111. Court of Overijssel 14 May 2014, ECLI:NL:RBOVE:2014:2667.
112. *Wet ter voorkoming van witwassen en financiering van terrorisme*, art. 1(1) jo. 1a (Dutch).
113. DNB & AFM, *Cryptos: recommendations for a regulatory framework* (https://www.dnb.nl/en/binaries/AFM-DNB%20Crypto%20Recommendations_tcm47-381603.pdf).
114. https://www.afm.nl/en/professionals/onderwerpen/ico%20 (available in English).
115. https://www.afm.nl/~/profmedia/files/onderwerpen/wwft/wwft-cryptocurrencies.pdf (Dutch).
116. *Implementatiewet wijziging vierde anti-witwasrichtlijn*, art. 23b and further (Dutch).
117. *Memorie van toelichting Implementatiewet wijziging vierde anti-witwasrichtlijn*, p. 10–11 (Explanatory Memorandum, Dutch).
118. Cryptoassets Taskforce: final report dated October 2018.
119. FCA Consultation Paper CP 19/3 "Guidance on Cryptoassets" dated January 2019.
120. Andrew Baily, BBC's Newsnight (Dec. 14, 2017).
121. To date, the status of cryptocurrencies as constituting "money" is yet to have been challenged in the UK courts. There therefore remains a possibility that the courts would be minded to conclude in the future that cryptocurrencies, such as Bitcoin, constitute money, in circumstances where they are more commonly and continuously being accepted as payment in exchange for goods and services. Having said that, as long as a cryptocurrency is not a "fiat currency" and is not pegged to the value of a fiat currency, it is unlikely to be subject to payments regulation as currently framed in the UK.
122. I.e., the UK implementation of the MLD4.
123. "Dear CEO – cryptoassets and financial crime", FCA, 2018.
124. Proceeds of Crime Act 2002 §§ 327–329 (UK).
125. *R v Teresko* (Sergejs) (Kingston Crown Court: HHJ Lodder QC, 11 October 2017, unreported).
126. High People's Court of Heilongjiang Province of China (2016), http://wenshu.court.gov.cn/Content/Content?DocID=ce26a599-64e9-44ab-96fd-b04617d482b4 (China).

127. People's Bank of China, Ministry of Indus. & Info. Tech., State Admin. for Indus. & Commerce, China Banking Reg. Comm'n, China Secs. Regulatory Commission, & China Ins. Regulatory Comm'n, Announcement on Preventing Token Fundraising Risks (关于防范代币发行融资风险的公告), (Sept. 4, 2017), http://www.cbrc.gov.cn/chinese/home/docView/BE5842392CFF4BD98B0F3DC9C2A4C540.html (China).
128. Zhou Xiaochuan, President of the People's Bank of China, talks about "Future regulations of the cryptocurrency", http://lianghui.people.com.cn/2018npc/n1/2018/0309/c418389-29858496.html (China).
129. China's regulation of cryptocurrency and ICO: Focus of the next step, Shanghai Securities News, 23 August 2018, http://www.nbd.com.cn/articles/2018-08-23/1248158.html (China).
130. Specifically, cryptocurrency is defined as something that: (i) can be used for payment to unspecified persons in the purchase or lease of goods, or paying consideration for the receipt of the provision of services; (ii) can be purchased from and sold to unspecified persons; (iii) has financial value; (iv) is recorded by electromagnetic means in electronic devices or other items; (v) is not the currency of Japan, foreign currencies, nor an "asset denominated in currencies"; and (vi) can be transferred using electronic data processing systems. Payment Services Act, Law No. 59 of 2009, art. 2, para. 5 (Japan).
131. *See* Art. 63-5 of the Amended Payment Services Act (Japan).
132. Law No. 22 of 2007. The PTCP was amended in April 2017 to include VCEOs in this definition.
133. *More Japanese Cryptocurrency Exchanges to Close*, Nikkei (Mar. 29, 2018), https://asia.nikkei.com/Markets/Currencies/More-Japanese-cryptocurrency-exchanges-to-close.
134. Australian Secs. & Inv. Comm'n, Information Sheet 225 (Sept. 2017), http://asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings/#shares (Austl.).
135. Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017 (Cth); *see also* Brad Vinning & Ruby Mackenzie-Harris, *Australia: the New Digital Era: Blockchain, Cryptocurrency, and ICOs – Part 3*, Mondaq (Feb. 26, 2018), http://www.mondaq.com/australia/x/676820/fin+tech/The+new+digital+era+Blockchain+cryptocurrency+and+ICOs+Part+3.
136. Digital Currency Exchange Providers – Guidance on AML/CTF Programs, AUSTRAC http://www.austrac.gov.au/digital-currency-exchange-providers (last visited Apr. 9, 2018, 10:00 EST).
137. *See* U.S. Dep't of Justice, Press Release, Ross Ulbricht, A/K/A "Dread Pirate Roberts", Sentenced In Manhattan Federal Court To Life In Prison, (May 29, 2015), https://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison.
138. Drug Enf't Admin., Dep't of Justice, 2017 National Drug Threat Assessment (DEA-DCT-DIR-040-17) 130 (Oct. 2017), https://www.dea.gov/docs/DIR-040-17_2017-NDTA.pdf.
139. Europol, Press Release, Illegal Network Used Cryptocurrencies and Cedit Cards to Launder More Than EUR 8 Million from Drug Trafficking (Apr. 9, 2018), https://www.europol.europa.eu/newsroom/news/illegal-network-used-cryptocurrencies-and-credit-cards-to-launder-more-eur-8-million-drug-trafficking.
140. *See* Quesito Antiriciclaggio n. 3-2018/B, Consiglio Nazionale del Notariato (Mar. 13, 2018), http://www.dirittobancario.it/sites/default/files/allegati/quesito_antiriciclaggio_n._3-2018-b.pdf (It.).
141. Zachary K. Goldman *et al*, *Terrorist Use of Virtual Currencies*, Center for a New American Security (May 2017), https://www.lawandsecurity.org/wp-content/uploads/2017/05/CLSCNASReport-TerroristFinancing-Final.pdf.
142. *Venezuela Says Launch of "Petro" Cryptocurrency Raised $735 Million*, Reuters (Feb. 20, 2018), https://www.reuters.com/article/us-crypto-currencies-venezuela/venezuela-says-launch-of-petro-cryptocurrency-raised-735-million-idUSKCN1G506F.
143. For example, the cryptocurrency Monero uses "stealth addresses", which are randomly generated for each individual transaction, and "ring confidential transactions", which conceals the amount being transacted. *See* Nicolas van Saberhagen, *Crypto-Note v. 2.0* (Monero White Paper) (Oct. 17, 2013), https://github.com/monero-project/research-lab/blob/master/whitepaper/whitepaper.pdf.
144. *E.g.*, FATF Recommendation 10 ("Customer Due Diligence"), https://www.cfatf-gafic.org/index.php/documents/fatf-40r/376-fatf-recommendation-10-customer-due-diligence.
145. 31 C.F.R. § 1010.313.
146. 31 U.S.C. § 5324.
147. Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States (Apr. 26, 2005), https://www.fincen.gov/sites/default/files/guidance/guidance04262005.pdf.
148. *Id*. at 3 (stating that "it is reasonable and appropriate for a banking organisation to insist that a money services business provide evidence of compliance with such requirements or demonstrate that it is not subject to such requirements").
149. Fed. Fin. Insts. Examination Council, *Nonbank Financial Institutions – Overview, Bank Secrecy Act Anti-Money Laundering Examination Manual*, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_091.htm (last visited Apr. 12, 2018).
150. *Id*.
151. An ACAMs white paper has raised concerns over the phenomenon of de-risking in crypto services, and of the potential fair banking services ramifications. "While consistent regulation is lacking, [VCEs] are being denied fair banking services because they are being 'de-risked' by [FIs]. The discrimination from fair banking services VCEs are facing is comparable to the medial marijuana industry. Unlike its high-risk counterpart, Fintech innovators operate in a field that is federally legal." Sherri Scott, *Cryptocurrency Compliance: An AML Perspective, ACAMS White Paper* (n.d.), http://files.acams.org/pdfs/2017/Cryptocurrency_Compliance_An_AML_Perspective_S.Scott.pdf.
152. FATF-modeled AML regimes include prohibitions on the acceptance of proceeds of a crime ("illicit proceeds"). *See*, *e.g.*, 18 U.S.C. §§ 1956–57.

Tracy French

Allen & Overy LLP
1101 New York Avenue, NW
Washington, D.C.
20005
USA

Tel: +1 202 683 3866
Email: tracy.french@allenovery.com
URL: www.allenovery.com

Tracy is an Associate in the Global Sanctions Group. Her practice focuses on economic sanctions as enforced by the U.S. Department of Treasury, Office of Foreign Assets Control ("**OFAC**") as well as anti-money laundering issues under the Bank Secrecy Act. Tracy advises global financial institutions and multinational companies on a broad spectrum of compliance and enforcement matters including internal investigations, voluntary disclosures, and the resolution of administrative and enforcement proceedings involving federal and state regulatory agencies and prosecutors. Tracy also counsels clients on anti-corruption issues and foreign investment in the United States regulated by the Committee on Foreign Investment in United States ("**CFIUS**").

Barbara Stettner

Allen & Overy LLP
1101 New York Avenue, NW
Washington, D.C.
20005
USA

Tel: +1 202 683 3850
Email: barbara.stettner@allenovery.com
URL: www.allenovery.com

Barbara is the Managing Partner of the Washington, D.C. office and is a member of the firm's global Executive Committee. Barbara's practice focuses on advising U.S. and foreign financial institutions on their regulatory and compliance obligations under the Securities Exchange Act of 1943, and the Bank Secrecy Act. Barbara represents global financial institutions and corporates on various financial services regulatory issues, including a strong focus on the application of anti-money laundering regimes on a cross-border basis to these global institutions.

She previously worked at the SEC's Division of Trading and Markets in the Office of the Chief Counsel and in the Office of Risk Management and Control. She also served in the Commission's Office of International Affairs together with the Financial Services Volunteer Corp, providing pro bono technical assistance to emerging markets on the creation and implementation of anti-money laundering regulations in Jordan, the UAE, Ukraine, Russia, and Romania.

ALLEN & OVERY

At a time of significant change in the legal industry, Allen & Overy is determined to continue leading the market as we have done throughout our 87-year history. To support our clients' international strategies, we have built a truly global network now spanning 44 offices in 31 countries. We have also developed strong ties with relationship law firms in over 100 countries where we do not have a presence. This network makes us one of the largest and most connected law firms in the world, with a global reach and local depth that is simply unrivalled. Global coverage in today's market does not simply mean having offices in important cities around the world. For us, it means combining our international resources and sector expertise to work on cross-border transactions directly in the markets and regions important to our clients.

Current titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Financial Services Disputes
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com