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

Daniel Holman

Barbara Stettner

Allen & Overy, LLP

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 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 as: (1) "a medium of exchange"; a (2) "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 time stamped 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 to 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

Despite calls for the adoption of global AML standards for cryptocurrency trading,[22] no such uniform rules have yet emerged. There has nonetheless been some convergence toward the FATF 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 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] 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.

European Union Regulatory Approach

The most recent European-level AML directive, the Fourth Money Laundering Directive ("**MLD4**"),[64] did not explicitly address cryptocurrency, and the European Commission has not interpreted its existing regulatory guidance to require extension of the MLD4 regime to cryptocurrencies.[65] As part of the development of the proposed Fifth Money Laundering Directive ("**MLD5**"),[66] however, the European Parliament and European Council reached an agreement in December 2017 that would extend AML obligations to firms operating centralised cryptocurrency exchanges or custodial wallet providers[67] for cryptocurrencies[68] by adding them to the definition of "obliged entities" contained in the existing directives.[69] These amendments would require EU Member States to subject those service providers to the same obligations as banks and other financial institutions under MLD4 – including CIP and beneficial ownership identification, KYC, transaction monitoring, and suspicious activity reporting – and will subject those providers to supervision by the competent national authorities for these areas.

Once MLD5 is published, Member States will have 18 months to implement most provisions into national law.[70] With publication of MLD5 anticipated to occur in mid-2018, national implementation of these requirements may be expected by late 2019 or early 2020.

While MLD5 is pending, some EU jurisdictions have 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[71] in compliance with MLD4 in 2017 (which was done via a legislative decree, "**AML4 Decree**"),[72] it simultaneously incorporated definitions for cryptocurrency consistent with the FATF-definition[73] and classified cryptocurrency service providers[74] that provide cryptocurrency-to-fiat conversion services as "non-financial intermediaries" regulated under the AML Decree.[75] Such service providers are consequently subject to Italian AML obligations,[76] including KYC,[77] record keeping and communications to the authorities,[78] suspicious transaction reporting,[79] and, as a consequence of the pseudo-anonymity of blockchain users, enhanced due diligence ("**EDD**").[80] 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[81] 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).[82] 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.[83]

Although Italy's investment services authority, CONSOB,[84] 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.[85] A 2015 Bank of Italy communication[86] 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.[87] 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.

(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**").[88] 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.[89] 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"[90] under the German Money Laundering Act ("**GWG**"),[91] transposing the MLD4 AML requirements.[92] 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.[93] 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 have not formally extended their AML regulation to cover cryptocurrency activities.

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**")[94] has provided assurance that VCE and wallet services for currency-like cryptocurrencies fall outside the scope of the DFSA[95] and, consequently, are in general not covered "institutions" for purposes of the Act for the Prevention of Money Laundering and Financing of Terrorism ("**Wwft**").[96] When MLD5 is implemented, however, the Wwft will extend to these entities as discussed above.[97] The Minister of Finance expects to complete the implementation of this amendment by the end of 2019.[98]

Although a lower court ruled in 2014 that Bitcoins do not themselves qualify as "common money",[99] as a practical matter many Dutch banks and other financial institutions have been reluctant to accept proceeds that derive from cryptocurrency exchange transactions if they cannot validate the origin of these funds. Additionally, cryptocurrencies that have the character of stocks or bonds would arguably also qualify as "securities" and therefore as "financial instruments" under the DFSA,[100] such that a provider of such a cryptocurrency or of investment services for such a cryptocurrency would be subject to the DFSA and, insofar as it relates to investment services, the Wwft.[101] However, to date there has been no formal action reaching such a conclusion.

(d) UK

In the UK, the prevailing view of regulators has been to treat cryptocurrencies as a commodity, rather than a currency or a security. On this basis, the UK Financial Conduct Authority ("**FCA**") chief executive Andrew Bailey recently confirmed 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.[102] The FCA has also confirmed that,[103] in its view, cryptocurrencies such as Bitcoin are not "specified investments" for the purposes of the Financial Services and Markets Act ("**FSMA**") 2000 (Regulated Activities) Order 2001.[104] Nonetheless, given the breadth of products that may be labelled as cryptocurrencies, there is a risk that some coins or tokens (including those issued as part of an ICO) may 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 ICOs may instead amount to a collective investment scheme under section 235 of the FSMA. Derivatives that reference a cryptocurrency are also capable of being regulated investments.[105]

Unless one of the regulated financial services regimes above is triggered, cryptocurrency activities are unlikely to currently fall within the scope of the UK Money Laundering Regulations 2017.[106] Changes currently proposed at the EU level (and supported by the UK Treasury) would result in cryptocurrency exchanges and custodian wallet providers' activities being within the scope of AML laws. Subject to Brexit, the UK will need to implement these provisions into national law and regulation within 18 months, meaning such amendments may apply by late 2019, if not sooner. Even if Brexit relieves the UK of these obligations before the MLD5 implementation deadline,[107] UK regulators or legislators may choose to design a bespoke regime to regulate and govern cryptocurrencies and their exchange, or to otherwise broaden existing financial services regulatory regimes to cover cryptocurrency activities.

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 constitute a predicate crime for certain money laundering offences under the Proceeds of Crime Act 2002.

Separate and apart from whether dealings with cryptocurrencies may implicate FI status under UK law, cryptocurrencies or the proceeds of their sale that could be the subject of a restraint order or confiscation order to the extent that they constitute criminal property under the Proceeds of Crime Act 2002 ("**POCA**"), and concealing or handling such criminal property could trigger the money laundering offences under POCA.[108] Moreover, where firms operate within the regulatory perimeter in breach of the FSMA general prohibition (e.g., by issuing security tokens without requisite FCA authorisation), such a breach would constitute a criminal offence, and thereby constitute a predicate crime for the primary money laundering offences under 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 crypto businesses, while Korea has yet to settle on a regulatory scheme of any kind.

(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.[109]

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.[110]

- 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.

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[111] and to create a registration requirement for "Virtual Currency Exchange Operators" ("**VCEOs**").[112] VCEO licences permit holders to engage in the exchange, purchase, sale, and safekeeping of cryptocurrencies on behalf of third parties, and to engage in ICOs subject to pre-approval by the FSA. 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.[113] Since licences were first issued to VCEOs on September 30, 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.[114]

(c) Korea

As at the time of writing, South Korea continues deliberations on reaching a comprehensive cryptocurrency regulatory scheme, resulting in a situation that some commentators have described as "a state of 'deliberate ambiguity'".[115] After initially legalising Bitcoin service providers for payments, transfers, and trades in July 2017,[116] cybersecurity and AML concerns led to the issuance of a ban on ICOs in September 2017.[117] Though subsequent remarks by public officials even suggested shutting down exchanges entirely, reports suggest that the ban has not been strictly enforced while the government's internal consultations continue[118] and that limitations will be lifted once a formal legal framework can be established.[119]

Because of the legal uncertainty regarding the future status of cryptocurrencies, the Korean Financial Services Commission ("**FSC**") has begun to regulate cryptocurrencies through its authority to regulate banks pursuant to its existing statutory powers. These measures, announced in January 2018, require cryptocurrency trading to occur through real-name bank accounts linked to cryptocurrency exchanges.[120] The FSC also introduced a mandatory "guideline" with respect to cryptocurrency-linked accounts to ensure bank compliance with AML.[121] Among other things, the guideline requires banks to "conduct [EDD] in transaction[s] with cryptocurrency exchanges to make sure users' money [is] in safe hands. The EDD requires banks to verify additional information for cryptocurrency exchanges: the purpose of financial transactions and the source of money; details about services that the exchanges provide; whether the exchanges are using real-name accounts; and whether the exchanges verify their users' identification".[122] The guideline also mandates banks to "refuse to offer accounts to cryptocurrency exchanges if they do not provide their users' ID information".[123]

(d) 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.[124] 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.[125] 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.[126]

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 FIs subject to AML requirements to stay abreast of new criminal uses.

- **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.[127]

- **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.
- **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.
- **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.

- **Placement**: The ability to rapidly and anonymously open anonymous accounts provides a low-risk means for criminal groups to convert and consolidate illicit cash.
- **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.[128] 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.[129] 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.
- **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 a 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.[130] 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.
- **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.[131] 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.[132]

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.[133]

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 fulfilment 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"[134] 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[135] and detection of structuring payments.[136] 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.[137] 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.[138] 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.[139] 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".[140]

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:

- **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?
- **Monitoring and reporting**: Does the customer have mechanisms in place for account monitoring and procedures in place for required reporting?
- **Geographic controls**: Is the service able to control the jurisdictions in which its services are accessed?
- **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.[141]

(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.[142] 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.

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/documents/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. See FATF 2015 Guidance, *supra* note 2, at 12.
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) cheque casher; (3) issuer of traveller's checks, money orders, or stored value; (4) seller or redeemer of traveller's checks, 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. 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].

65. *Id.* Specifically, the European Parliament and the Council of the European Union determined that the rules and regulation of the MLD4 do 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].

66. Proposal for a Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849, *supra* note 66.

67. *I.e.*, wallets that hold the customer's private keys, and therefore have effective custody of the customer's blockchain account.

68. The proposal for MLD5 contains the following definition of virtual currencies: "'virtual currencies' means a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically". Proposal for a Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849, *supra* note 66.

69. EU Directive 2015/849, *supra* note 65.

70. More time may be permitted for provisions which have different transposition deadlines.

71. 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.).

72. 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.).

73. 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).

74. 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).

75. *Id.* art. 3 ¶ 5(i).

76. *Id.* art. 3.

77. *Id.* arts. 17–30.

78. *Id.* arts. 31–34.

79. *Id.* arts. 35–41.

80. 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.

81. Held by the Italian Organization of Agents and Mediators.

82. AML4 Decree, *supra* note 73, at art. 8 (by amending Legislative Decree n.141 of 13 Aug. 2010 art. 17-*bis*.).

83. 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.).

84. *Commissione Nazionale per le Società e la Borsa*.

85. 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.

86. *Banca D'Italia Eurosistem*, *Avvertenza sull'utilizzo delle cosiddette* "*valute virtuali*", 30 Jan. 2015 (It.).

87. *See* Legislative Decree n. 385 of 1 Sept. 1993 arts. 130–131, 131-*ter*, 166 (It.).

88. 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.).

89. Likewise, the creation of new cryptocurrency by solving complex mathematical computational tasks (mining) does not constitute a regulated activity according to the KWG.

90. "*Verpflichtete*".
91. *Geldwäschegesetz* [GwG] [Money Laundering Act], Aug. 13, 2008 at §§ 2(1)(1)-(2) (Ger.).
92. *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.).
93. 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.).
94. *Beantwoording schriftelijke Kamervragen Nijboer over het gebruik van en toezicht op nieuwe digitale betaalmiddelen zoals de Bitcoin*, FM/2013/1939 U (19 Dec. 2013) [hereinafter FM/2013/1939 U] (Neth.).
95. *Id.*
96. *Wet ter voorkoming van witwassen en financiering van* terrorisme Aug. 1, 2008, art. 1, ¶ 1, sub a (Neth.) [hereinafter Wwft].
97. *I.e.*, VCEs and wallet providers offering custodial services of credentials necessary to access virtual currencies.
98. Chairman of the House of Representatives of the States General, *Letter on Cryptocurrency Developments* (8 Mar. 2018), 2018-0000033278, https://www.rijksoverheid.nl/documenten/kamerstukken/2018/03/08/achtergrond-en-overige-informatie-over-cryptovaluta (Neth.).
99. Court of Overijssel 14 May 2014, ECLI:NL:RBOVE:2014:2667.
100. "*Effect*", as defined in article 1:1 of the DFSA. FM/2013/1939 U, *supra* note 95, art. 1:1. Specifically, such securities would potentially be a "*financieel instrument*", as defined in article 1:1 of the DFSA). *Id.*
101. Wwft, *supra* note 97, art. 1, ¶ 1, sub a.
102. Andrew Baily, BBC's Newsnight (Dec. 14, 2017).
103. Letter from Andrew Bailey, FCA, to Nicky Morgan, MP, Treasury Select Committee (dated Jan. 30, 2018).
104. Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (UK).
105. To date, the status of cryptocurrencies 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, for so 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.
106. *I.e.*, the UK implementation of the MLD4.
107. The UK government recently established a crypto-assets taskforce, consisting of the UK Treasury, the Bank of England, and the UK Financial Conduct Authority, to study the issue and make legislative proposals.
108. Proceeds of Crime Act 2002 §§ 327–329 (UK).
109. High People's Court of Heilongjiang Province of China (2016), http://wenshu.court.gov.cn/Content/Content?DocID=ce26a599-64e9-44ab-96fd-b04617d482b4 (China).
110. 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).
111. 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).
112. *See* Art. 63-5 of the Amended Payment Services Act (Japan).
113. Law No. 22 of 2007. The PTCP was amended in April 2017 to include VCEOs in this definition.
114. *More Japanese Cryptocurrency Exchanges to Close*, Nikkei (Mar. 29, 2018), https://asia.nikkei.com/Markets/Currencies/More-Japanese-cryptocurrency-exchanges-to-close.
115. Andrew Salmon, *Korean Cryptocurrency Market Faces New Regulatory Risk*, Asia Times (Mar. 19, 2018), http://www.atimes.com/article/korean-cryptocurrency-market-faces-new-regulatory-risk/ (quoting Ahn Chan-sik, who leads the Technology and Communications practice at Hwang, Mok, Park).
116. Son Ji-hyoung, *Bills Move to Give Bitcoin Legal Grounds*, Korea Herald (July 3, 2017), http://www.koreaherald.com/view.php?ud=20170703000867.
117. Forbes Tech. Council, *How Will The China And South Korea ICO Bans Impact Cryptocurrencies?*, Forbes (Dec. 11, 2017), https://www.forbes.com/sites/forbestechcouncil/2017/12/11/how-will-the-china-and-south-korea-ico-bans-impact-cryptocurrencies/#44fe17ef5124.
118. Dahee Kim & Ju-min Park, *South Korea Keeps Investors Guessing on Cryptocurrency Regulation*, Reuters (Feb. 28, 2018), https://www.reuters.com/article/us-malaysia-cenbank-cybersecurity-incide/malaysian-central-bank-says-foiled-attempted-cyber-heist-idUSKBN1H50YF (citing government statements that further consultations are needed before the government will reach a final conclusion as to how to regulate the sector).
119. Eli Meixler, *It Looks Like South Korea is Planning to Allow ICOs and Regulate Crypto Trading After All*, Fortune (Mar. 13, 2018), http://fortune.com/2018/03/12/south-korea-cryptocurrency-ico/.
120. Press Release, South Korean Fin. Servs. Comm'n, Financial Measures to Curb Speculation in Cryptocurrency Trading (Jan. 23, 2018), http://www.fsc.go.kr/downManager?bbsid=BBS0048&no=123388 (S. Kor.).
121. *Id.*
122. *Id.*
123. *Id.*
124. Australian Secs. & Inv. Comm'n, Information Sheet 225 (Sept. 2017), http://asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings/#shares (Austl.).
125. 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.

126. 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).
127. *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.
128. 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.
129. Europol, Press Release, Illegal Network Used Cryptocurrencies and Credit 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.
130. *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.).
131. 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.
132. *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.
133. 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.
134. *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.
135. 31 C.F.R. § 1010.313.
136. 31 U.S.C. § 5324.
137. 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.
138. *Id*. at 3 (stating that "it is reasonable and appropriate for a banking organization to insist that a money services business provide evidence of compliance with such requirements or demonstrate that it is not subject to such requirements").
139. 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).
140. *Id*.
141. 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.
142. FATF-modelled AML regimes include prohibitions on the acceptance of proceeds of a crime ("illicit proceeds"). *See*, *e.g.*, 18 U.S.C. §§ 1956–57.

Acknowledgment

The authors wish to thank the following attorneys for their significant contributions to this chapter: Jane Jiang, Tiantian Wang and Jason Song (China); Dennis Kunschke (Germany); Giovanni Battista Donato, Emanuela Semino, and Amilcare Sada (Italy); Neyah van der Aa, Robin van Duijnhoven, and Daphne van der Houwen (the Netherlands); Ben Regnard-Weinrabe and Heenal Vasu (UK); and Sam Brown, Bill Satchell, Justin Cooke, Lindsay Kennedy, Derek Manners, and Chelsea Pizzola (U.S.).

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

Tel: +1 202 683 3853
Email: daniel.holman@allenovery.com
URL: www.allenovery.com

Daniel is an associate in the Investigations and Litigation practice group in the firm's Washington, D.C. office. His practice includes supporting clients in the conduct of multijurisdictional internal investigations and advocating for them in contentious regulatory proceedings in the areas of competition, anticorruption, anti-money laundering, government procurement, pay-to-play, campaign finance, and lobbying regulation. Daniel also advises clients on compliance obligations in these areas. Prior to joining Allen & Overy, Daniel was a Visiting Fellow at the UNAM Legal Research Institute in Mexico City.

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.