

Overview Report: FATF Publications on Virtual Assets

A. Scope of Overview Report

1. This overview report sets out information regarding publications by the Financial Action Task Force (“FATF”) and the United States Department of Justice relating to virtual assets. Its purpose is to provide background and context to evidence to viva voce evidence led during Commission hearings.

B. The FATF Documents

2. FATF’s Recommendation 15 states:

15. New technologies

Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

3. Recommendation 15 was expanded in 2018 to provide that ‘To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations’.¹

4. The FATF report, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, published June 2014, is attached as Appendix “A”.

5. The *Guidance for a Risk-Based Approach: Virtual Currencies* was published in June 2015 and is attached as Appendix “B”.

¹ Financial Action Task Force, *International Standards on Combatting Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations* (Paris: FATF, October 2020) online: <<http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>>

6. The document, “Regulation of virtual assets” was published in 2018 and is attached as Appendix “C”.

7. FATF clarified member state obligations with respect to VA regulation in June 2019 by adopting an Interpretive Note to Recommendation 15 (INR.15). The text of INR.15 is attached as Appendix “D”.

8. The updated 2019 Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, is attached as Appendix “E”.

9. In July 2020, FATF published “12 Month Review of Revised FATF Standards - Virtual Assets and VASPs”, which is attached as Appendix “F”.

10. In September 2020, FATF published “Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets”, which is attached as Appendix “G”.

C. United States Department of Justice Documents

11. Attached as Appendix “H” is “The Report of the Attorney General’s Cyber Digital Task Force”, published in October 2020.



FATF REPORT

Virtual Currencies Key Definitions and Potential AML/CFT Risks

June 2014



FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

www.fatf-gafi.org

© 2014 FATF/OECD. All rights reserved.

No reproduction or translation of this publication may be made without prior written permission.

Applications for such permission, for all or part of this publication, should be made to the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France

(fax: +33 1 44 30 61 37 or e-mail: contact@fatf-gafi.org).

Photocredits coverphoto: ©Thinkstock

CONTENTS

INTRODUCTION.....	3
KEY DEFINITIONS:.....	3
Virtual Currency	4
Convertible Versus Non-Convertible Virtual Currency	4
Centralised Versus Non-Centralised Virtual Currencies.....	5
Virtual Currency System Participants.....	7
LEGITIMATE USES.....	8
POTENTIAL RISKS	9
LAW ENFORCEMENT ACTIONS INVOLVING VIRTUAL CURRENCY	10
Liberty Reserve.....	10
Silk Road	11
Western Express International.....	12
NOTES	13
BIBLIOGRAPHY AND SOURCES	15

ACRONYMS

AML/CFT	Anti-money laundering / countering the financing of terrorism
ECB	European Central Bank
FATF	Financial Action Task Force
NPPS Guidance	Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services

VIRTUAL CURRENCIES - KEY DEFINITIONS AND POTENTIAL AML/CFT RISKS¹

INTRODUCTION

As decentralised, math-based virtual currencies—particularly Bitcoin²—have garnered increasing attention, two popular narratives have emerged: (1) virtual currencies are the wave of the future for payment systems; and (2) virtual currencies provide a powerful new tool for criminals, terrorist financiers and other sanctions evaders to move and store illicit funds, out of the reach of law enforcement and other authorities.³ Against this backdrop, this paper builds on the 2013 New Payment Products and Services (NPPS) Guidance (FATF, 2013) by suggesting a conceptual framework for understanding and addressing the anti-money laundering / countering the financing of terrorism (AML/CFT) risks associated with one kind of internet-based payment system: virtual currencies. Specifically, the paper proposes a common definitional vocabulary that clarifies what virtual currency is and classifies the various types of virtual currency, based on their different business models and methods of operation,⁴ and identifies the participants in typical virtual currency systems. It also applies risk factors set forth in Section IV (A) of the 2013 NPPS Guidance to specific types of virtual currencies to identify potential risks; describes some recent investigations and enforcement efforts involving virtual currency; and presents a sample of jurisdictions' current regulatory approaches to virtual currency.

While the 2013 NPPS Guidance broadly addressed internet-based payment services, it did not define “digital currency,” “virtual currency,” or “electronic money.” Nor did it focus on virtual currencies, as distinct from internet-based payment systems that facilitate transactions denominated in real money (fiat or national currency) (e.g., Pay-Pal, Alipay, or Google Checkout). It also did not address decentralised convertible virtual currencies, such as Bitcoin. The 2013 Guidance also notes that, “[g]iven the developing nature of alternate online currencies, the FATF may consider further work in this area in the future” (2013 NPPS Guidance, p. 11, para. 29). A short-term typologies project on this basis was initiated with the following objectives:

- develop a risk-matrix for virtual currencies (or perhaps, more broadly, for both virtual currencies and e-money);
- promote fuller understanding of the parties involved in convertible virtual currency systems and the way virtual currency can be used to operate payment systems; and
- stimulate a discussion on implementing risk-based AML/CFT regulations in this area.

This typologies project may lead to policy work by the FATF, e.g. the issuance of supplemental guidance for applying a risk-based approach to virtual currencies that would incorporate the proposed vocabulary and risk-matrix developed by the typologies project and explain how specific FATF Recommendations apply in the context of virtual currency.

KEY DEFINITIONS:

A common set of terms reflecting how virtual currencies operate is a crucial first step to enable government officials, law enforcement, and private sector entities to analyse the potential AML/CFT

risks of virtual currency as a new payment method. As regulators and law enforcement officials around the world begin to grapple with the challenges presented by virtual currencies, it has become apparent that we lack a common vocabulary that accurately reflects the different forms virtual currency may take. The following set of terms is intended to aid discussion between FATF members. It is important to note that this vocabulary may change as virtual currency evolves and as regulators and law enforcement/government officials continue to consider the challenges virtual currencies present. Nevertheless, the proposed vocabulary aims to provide a common language for developing conceptual tools to help us better understand how virtual currencies operate and the risks and potential benefits they offer.

VIRTUAL CURRENCY

Virtual currency is a digital representation⁵ of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment)⁶ in any jurisdiction.⁷ It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency. Virtual currency is distinguished from **fiat currency** (a.k.a. “**real currency**,” “**real money**,” or “**national currency**”), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from **e-money**, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency—i.e., it electronically transfers value that has legal tender status.

Digital currency can mean a digital representation of either virtual currency (non-fiat) or e-money (fiat) and thus is often used interchangeably with the term “virtual currency”. In this paper to avoid confusion, only the terms “virtual currency” or “e-money” are used.

CONVERTIBLE VERSUS NON-CONVERTIBLE VIRTUAL CURRENCY

This paper proposes dividing virtual currency into two basic types: convertible and non-convertible virtual currency.⁸ Although the paper uses “non-convertible” and “closed”, and “convertible” and “open” as synonyms, it should be emphasised that the notion of “convertible currency” does not in any way imply an ex officio convertibility (e.g. in the case of gold standard), but rather a de facto convertibility (e.g. because a market exists). Thus, a virtual currency is “convertible” only as long as some private participants make offers and others accept them, since the “convertibility” is not guaranteed at all by law.

Convertible (or open) virtual currency has an equivalent value in real currency and can be exchanged back-and-forth for real currency.⁹ Examples include: Bitcoin; e-Gold (defunct); Liberty Reserve (defunct); Second Life Linden Dollars; and WebMoney.¹⁰

Non-convertible (or closed) virtual currency is intended to be specific to a particular virtual domain or world, such as a Massively Multiplayer Online Role-Playing Game (MMORPG) or Amazon.com, and under the rules governing its use, cannot be exchanged for fiat currency. Examples include: Project Entropia Dollars; Q Coins; and World of Warcraft Gold.

It should be noted that even where, under the terms set by the administrator, a non-convertible currency is officially transferrable only within a specific virtual environment and is not convertible, it is possible that an unofficial, secondary black market may arise that provides an opportunity to exchange the “non-convertible” virtual currency for fiat currency or another virtual currency. Generally, the administrator will apply sanctions (including termination of membership and/or forfeiture of remaining virtual currency) to those seeking to create or use a secondary market, contrary to the rules of the currency.¹¹ Development of a robust secondary black market in a particular “non-convertible” virtual currency may, as a practical matter, effectively transform it into a convertible virtual currency. A non-convertible characterisation is thus not necessarily static.

CENTRALISED VERSUS NON-CENTRALISED VIRTUAL CURRENCIES

All non-convertible virtual currencies are centralised: by definition, they are issued by a central authority that establishes rules making them non-convertible. In contrast, convertible virtual currencies may be either of two sub-types: centralised or decentralised.

Centralised Virtual Currencies have a single administrating authority (**administrator**)—i.e., a third party¹² 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). The exchange rate for a convertible virtual currency may be either **floating**—i.e., determined by market supply and demand for the virtual currency--or **pegged**—i.e., fixed by the administrator at a set value measured in fiat currency or another real-world store of value, such as gold or a basket of currencies. Currently, the vast majority of virtual currency payments transactions involve centralised virtual currencies. Examples: E-gold (defunct); Liberty Reserve dollars/euros (defunct); Second Life “Linden dollars”; PerfectMoney; WebMoney “WM units”; and World of Warcraft gold.

Decentralised Virtual Currencies (a.k.a. crypto-currencies) are distributed¹³, open-source, math-based peer-to-peer virtual currencies that have no central administrating authority, and no central monitoring or oversight. Examples: Bitcoin; Litecoin; and Ripple.¹⁴

Cryptocurrency refers to a math-based, decentralised convertible virtual currency that is protected by cryptography.—i.e., it incorporates principles of cryptography to implement a distributed, decentralised, secure information economy. Cryptocurrency relies on public and private keys to transfer value from one person (individual or entity) to another, and must be cryptographically signed each time it is transferred. The safety, integrity and balance of cryptocurrency ledgers is ensured by a network of mutually distrustful parties (in Bitcoin, referred to as miners) who protect the network in exchange for the opportunity to obtain a randomly distributed fee (in Bitcoin, a small number of newly created bitcoins, called the “block reward” and in some cases, also transaction fees paid by users as a incentive for miners to include their transactions in the next block). Hundreds of cryptocurrency specifications have been defined, mostly derived from Bitcoin, which uses a proof-of-work system to validate transactions and maintain the block chain. While Bitcoin provided the first fully implemented cryptocurrency protocol, there is growing interest in developing alternative, potentially more efficient proof methods, such as systems based on proof-of-stake.

Bitcoin, launched in 2009, was the first decentralised convertible virtual currency, and the first cryptocurrency. Bitcoins are units of account composed of unique strings of numbers and letters

that constitute units of the currency and have value only because individual users are willing to pay for them. Bitcoins are digitally traded between users with a high degree of anonymity and can be exchanged (purchased or cashed out) into US dollars, Euros, and other fiat or virtual currencies. Anyone can download the free, open-source software from a website to send, receive, and store bitcoins and monitor Bitcoin transactions. Users can also obtain Bitcoin addresses, which function like accounts, at a Bitcoin exchanger or online wallet service. Transactions (fund flows) are publicly available in a shared transaction register and identified by the Bitcoin address, a string of letters and numbers that is not systematically linked to an individual. Therefore, Bitcoin is said to be “pseudo-anonymous”. Bitcoin is capped at 21 million bitcoins (but each unit could be divided in smaller parts), projected to be reached by 2140.¹⁵ As of April 2, 2014, there were over 12-and-a-half million bitcoins, with total value of slightly more than USD 5.5 billion, based on the average exchange rate on that date.

Altcoin refers to math-based decentralised convertible virtual currency other than bitcoins, the original such currency. Current examples include Ripple; PeerCoin, Lite-coin; zerocoin; anoncoin and dogecoin. One popular exchanger, Cryptsy, would reportedly exchange over 100 different virtual currencies (as of 2 April 2014). (Popper, N., 2013)

Anonymiser (anonymising tool) refers to tools and services, such as darknets and mixers, designed to obscure the source of a Bitcoin transaction and facilitate anonymity. (Examples: Tor (darknet); Dark Wallet (darknet); Bitcoin Laundry (mixer)).

Mixer (laundry service, tumbler) is a type of anonymiser that obscures the chain of transactions on the blockchain by linking all transactions in the same bitcoin address and sending them together in a way that makes them look as if they were sent from another address. A mixer or tumbler sends transactions through a complex, semi-random series of dummy transactions that makes it extremely difficult to link specific virtual coins (addresses) with a particular transaction. Mixer services operate by receiving instructions from a user to send funds to a particular bitcoin address. The mixing service then “comingles” this transaction with other user transactions, such that it becomes unclear to whom the user intended the funds to be directed. (Examples: Bitmixer.io; SharedCoin; Blockchain.info; Bitcoin Laundry; Bitlaunder; Easycoin).

Tor (originally, The Onion Router) is an underground distributed network of computers on the Internet that conceals the true IP addresses, and therefore the identities of the network’s users, by routing communications/transactions through multiple computers around the world and wrapping them in numerous layers of encryption. Tor makes it very difficult to physically locate computers hosting or accessing websites on the network. This difficulty can be exacerbated by use of additional tumblers or anonymisers on the Tor network. Tor is one of several underground distributed computer networks, often referred to as darknets, cypherspace, the Deep web, or anonymous networks, which individuals use to access content in a manner designed to obscure their identity and associated Internet activity.

Dark Wallet is a browser-based extension wallet, currently available on Chrome (and potentially on Firefox), that seeks to ensure the anonymity of Bitcoin transactions by incorporating the following features: auto-anonymiser (mixer); decentralised trading; uncensorable crowd funding platforms; stock platforms and information black markets; and decentralised market places similar to Silk Road.

Cold Storage refers to an offline Bitcoin wallet—i.e., a Bitcoin wallet that is not connected to the Internet. Cold storage is intended to help protect the stored virtual currency against hacking and theft.

Hot Storage refers to an online bitcoin wallet. Because it is connected to the Internet, hot storage is more vulnerable to hacking/theft than cold storage.

Local Exchange Trading System (LETS) is a locally organised economic organisation that allows members to exchange goods and services with others in the group. LETS use a locally created currency to denominate units of value that can be traded or bartered in exchange for goods or services. Theoretically, bitcoins could be adopted as the local currency used within a LETS. (Examples: Ithica Dollars; Mazacoin).

VIRTUAL CURRENCY SYSTEM PARTICIPANTS

An **exchanger (also sometimes called a virtual currency exchange)** is a person or entity engaged as a business in the exchange of virtual currency for real currency, funds, or other forms of virtual currency and also precious metals, and vice versa, for a fee (commission). Exchangers generally accept a wide range of payments, including cash, wires, credit cards, and other virtual currencies, and can be administrator-affiliated, non-affiliated, or a third party provider. Exchangers can act as a bourse or as an exchange desk. Individuals typically use exchangers to deposit and withdraw money from virtual currency accounts.

An **administrator** is a person or entity engaged as a business in **issuing** (putting into circulation) a centralised virtual currency, establishing the rules for its use; maintaining a central payment ledger; and who has the authority to **redeem** (withdraw from circulation) the virtual currency.

A **user** is a person/entity who obtains virtual currency and uses it to purchase real or virtual goods or services or send transfers in a personal capacity to another person (for personal use), or who holds the virtual currency as a (personal) investment. Users can obtain virtual currency in several ways. For example, they can (1) purchase virtual currency, using real money (from an exchanger or, for certain centralised virtual currencies, directly from the administrator/issuer); (2) engage in specific activities that earn virtual currency payments (e.g., respond to a promotion, complete an online survey, provide a real or virtual good or service); (3) with some decentralised virtual currencies (e.g., Bitcoin), self-generate units of the currency by "mining" them (see definition of miner, below), and receive them as gifts, rewards, or as part of a free initial distribution.

A **miner** is an individual or entity that participates in a decentralised virtual currency network by running special software to solve complex algorithms in a distributed proof-of-work or other distributed proof system used to validate transactions in the virtual currency system. Miners may be users, if they self-generate a convertible virtual currency solely for their own purposes, e.g., to hold for investment or to use to pay an existing obligation or to purchase goods and services. Miners may also participate in a virtual currency system as exchangers, creating the virtual currency as a business in order to sell it for fiat currency or other virtual currency.

Virtual currency wallet is a means (software application or other mechanism/medium) for holding, storing and transferring bitcoins or other virtual currency.

A wallet provider is an entity that provides a virtual currency wallet (i.e., a means (software application or other mechanism/medium) for holding, storing and transferring bitcoins or other virtual currency). A wallet holds the user’s private keys, which allow the user to spend virtual currency allocated to the virtual currency address in the block chain. A wallet provider facilitates participation in a virtual currency system by allowing users, exchangers, and merchants to more easily conduct the virtual currency transactions. The wallet provider maintains the customer’s virtual currency balance and generally also provides storage and transaction security. For example, beyond providing bitcoin addresses, the wallet may offer encryption; multiple key (multi-key) signature protection, backup/cold storage; and mixers. All Bitcoin wallets can interoperate with each other. Wallets can be stored both online (“hot storage”) or offline (“cold storage”). (Examples: Coinbase; Multibit; Bitcoin Wallet).

In addition, various **other entities** may participate in a virtual currency system and may be affiliated with or independent of exchangers and/or administrators. These include web **administration service providers (a.k.a. web administrators)**; **third party payments senders** facilitating merchant acceptance; **software developers**; and **application providers** (some of the “other entities” listed in this paragraph may already fall into one of the categories above.). Applications and software development can be for legitimate purposes—e.g., to increase ease of merchant acceptance and customer payments or to respond to legitimate privacy concerns—or for illicit purposes—e.g., a mixer developer/operator can target illicit users with products designed to avoid regulatory and law enforcement scrutiny.

It must be emphasised that this list of participants is not exhaustive. Moreover, given the rapid development of virtual currency technologies and business models, additional participants could arise within virtual currency systems and pose potential AML/CFT risks.

Taxonomy of Virtual Currencies

	Centralised	Decentralised
Convertible	Administrator, exchangers, users; third-party ledger; can be exchanged for fiat currency. Example: WebMoney	Exchangers, users (no administrator); no Trusted Third-Party ledger; can be exchanged for fiat currency. Example: Bitcoin
Non-convertible	Administrator, exchangers, users; third-party ledger; cannot be exchanged for fiat currency. Example: World of Warcraft Gold	Does not exist

LEGITIMATE USES

Like other new payment methods, virtual currency has legitimate uses, with prominent venture capital firms investing in virtual currency start-ups. Virtual currency has the potential to improve

payment efficiency and reduce transaction costs for payments and fund transfers. For example, Bitcoin functions as a global currency that can avoid exchange fees, is currently processed with lower fees/charges than traditional credit and debit cards, and may potentially provide benefit to existing online payment systems, like Paypal.¹⁶ Virtual currency may also facilitate micro-payments, allowing businesses to monetise very low-cost goods or services sold on the Internet, such as one-time game or music downloads. At present, as a practical matter, such items cannot be sold at an appropriately low per/unit cost because of the higher transaction costs associated with e.g., traditional credit and debit. Virtual currency may also facilitate international remittances and support financial inclusion in other ways, as new virtual currency-based products and services are developed that may potentially serve the under- and un-banked. Virtual currency - notably, Bitcoin - may also be held for investment. These potential benefits need to be carefully analysed, including whether claimed cost advantages will remain if virtual currency becomes subject to regulatory requirements similar to those that apply to other payments methods, and/or if exchange fees for cashing out into fiat currency are factored in, and whether volatility, consumer protection and other factors¹⁷ limit their potential for financial inclusion.

POTENTIAL RISKS

Convertible virtual currencies that can be exchanged for real money or other virtual currencies are potentially vulnerable to money laundering and terrorist financing abuse for many of the reasons identified in the 2013 NPPS Guidance. First, they may allow greater anonymity than traditional non-cash payment methods. Virtual currency systems can be traded on the Internet, are generally characterised by non-face-to-face customer relationships, and may permit anonymous funding (cash funding or third-party funding through virtual exchangers that do not properly identify the funding source). They may also permit anonymous transfers, if sender and recipient are not adequately identified.

Decentralised systems are particularly vulnerable to anonymity risks. For example, by design, Bitcoin addresses, which function as accounts, have no names or other customer identification attached, and the system has no central server or service provider. The Bitcoin protocol does not require or provide identification and verification of participants or generate historical records of transactions that are necessarily associated with real world identity. There is no central oversight body, and no AML software currently available to monitor and identify suspicious transaction patterns. Law enforcement cannot target one central location or entity (administrator) for investigative or asset seizure purposes (although authorities can target individual exchangers for client information that the exchanger may collect). It thus offers a level of potential anonymity impossible with traditional credit and debit cards or older online payment systems, such as PayPal.

Virtual currency's global reach likewise increases its potential AML/CFT risks. Virtual currency systems can be accessed via the Internet (including via mobile phones) and can be used to make cross-border payments and funds transfers. In addition, virtual currencies commonly rely on complex infrastructures that involve several entities, often spread across several countries, to transfer funds or execute payments. This segmentation of services means that responsibility for AML/CFT compliance and supervision/enforcement may be unclear. Moreover, customer and transaction records may be held by different entities, often in different jurisdictions, making it more

difficult for law enforcement and regulators to access them. This problem is exacerbated by the rapidly evolving nature of decentralised virtual currency technology and business models, including the changing number and types/roles of participants providing services in virtual currency payments systems. And importantly, components of a virtual currency system may be located in jurisdictions that do not have adequate AML/CFT controls. Centralised virtual currency systems could be complicit in money laundering and could deliberately seek out jurisdictions with weak AML/CFT regimes. Decentralised convertible virtual currencies allowing anonymous person-to-person transactions may seem to exist in a digital universe entirely outside the reach of any particular country.

LAW ENFORCEMENT ACTIONS INVOLVING VIRTUAL CURRENCY

Law enforcement is already seeing cases that involve the abuse of virtual currency for money laundering purposes. Examples include:

LIBERTY RESERVE

In what is to date the largest online money-laundering case in history, in May 2013, the US Department of Justice charged Liberty Reserve, a Costa Rica-based money transmitter, and seven of its principals and employees with operating an unregistered money transmitter business and money laundering for facilitating the movement of more than 6 billion USD in illicit proceeds. In a coordinated action, the Department of the Treasury identified Liberty Reserve as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act, effectively cutting it off from the US financial system.

Established in 2006, Liberty Reserve was designed to avoid regulatory and law enforcement scrutiny and help criminals distribute, store, and launder the proceeds of credit card fraud, identity theft, investment fraud, computer hacking, narcotics trafficking, and child pornography by enabling them to conduct anonymous and untraceable financial transactions. Operating on an enormous scale, it had more than a million users worldwide, including more than 200 000 in the United States, and handled approximately 55 million transactions, almost all of which were illegal. It had its own virtual currency, Liberty Dollars (LR), but at each end, transfers were denominated and stored in fiat currency (US dollars).

To use LR currency, a user opened an account through the Liberty Reserve website. While Liberty Reserve ostensibly required basic identifying information, it did not validate identities. Users routinely established accounts under false names, including blatantly criminal names (“Russia Hackers,” “Hacker Account,” “Joe Bogus”) and blatantly false addresses (“123 Fake Main Street, Completely Made Up City, New York”). To add a further layer of anonymity, Liberty Reserve required users to make deposits and withdrawals through recommended third-party exchangers—generally, unlicensed money transmitting businesses operating in Russia, and in several countries without significant governmental money laundering oversight or regulation at that time, such as Malaysia, Nigeria, and Vietnam. By avoiding direct deposits and withdrawals from users, Liberty Reserve evaded collecting information about them through banking transactions or other activity that would create a central paper trail. Once an account was established, a user could conduct transactions with other Liberty Reserve users by transferring LR from his or her account to other

users, including front company “merchants” that accepted LR as payment. For an extra “privacy fee” (75 US cents per transaction), users could hide their Liberty Reserve account numbers when transferring funds, making the transfers completely untraceable. After learning it was being investigated by US law enforcement, Liberty Reserve pretended to shut down in Costa Rica but continued to operate through a set of shell companies, moving millions through their accounts in Australia, Cyprus, China, Hong Kong, Morocco, Russia, Spain and elsewhere.¹⁸

SILK ROAD

In September 2013, the US Department of Justice unsealed a criminal complaint charging the alleged owner and operator of Silk Road, a hidden website designed to enable its users to buy and sell illegal drugs, weapons, stolen identity information and other unlawful goods and services anonymously and beyond the reach of law enforcement, with narcotics trafficking, computer hacking, and money laundering conspiracies. The Justice Department also seized the website and approximately 173 991 bitcoins, worth more than USD 33.6 million at the time of the seizure, from seized computer hardware. The individual was arrested in San Francisco in October and indicted in February 2014; the investigation is ongoing.

Launched in January 2011, Silk Road operated as a global black-market cyber bazaar that brokered anonymous criminal transactions and was used by several thousand drug dealers and other unlawful vendors to distribute unlawful goods and services to over a hundred thousand buyers, a third of whom are believed to have been in the United States. It allegedly generated total sales revenue of approximately USD 1.2 billion (more than 9.5 million bitcoins) and approximately USD 80 million (more than 600 000 bitcoins) in commissions for Silk Road. Hundreds of millions of dollars were laundered from these illegal transactions (based on bitcoin value as of dates of seizure). Commissions ranged from 8 to 15 percent of total sales price.

Silk Road achieved anonymity by operating on the hidden Tor network and accepting only bitcoins for payment. Using bitcoins as the exclusive currency on Silk Road allowed purchasers and sellers to further conceal their identity, since senders and recipients of peer-to-peer (P2P) bitcoin transactions are identified only by the anonymous bitcoin address/account. Moreover, users can obtain an unlimited number of bitcoin addresses and use a different one for each transaction, further obscuring the trail of illicit proceeds. Users can also employ additional “anonymisers,” beyond the tumbler service built into Silk Road transactions (see discussion below).

Silk Road’s payment system functioned as an internal Bitcoin bank, where every Silk Road user had to hold an account in order to conduct transactions on the site. Every Silk Road user had at least one Silk Road Bitcoin address (and potentially thousands) associated with the user’s Silk Road account, stored on wallets maintained on servers controlled by Silk Road. To make a purchase, a user obtained bitcoins (typically through a Bitcoin exchanger) and sent them to a Bitcoin address associated with his or her Silk Road account to fund the account. When a purchase was made, Silk Road transferred the user’s bitcoins to an escrow account it maintained, pending completion of the transaction, and then transferred the user’s / buyer’s bitcoins from the escrow account to the vendor’s Silk Road Bitcoin address. As a further step, Silk Road employed a “tumbler” for every purchase, which, as the site explained, “sen[t] all payments through a complex, semi-random series

of dummy transactions ... --making it nearly impossible to link your payment with any [bit]coins leaving the site.”¹⁹

WESTERN EXPRESS INTERNATIONAL

An eight-year investigation of a multinational, Internet-based cybercrime group, the Western Express Cybercrime Group, resulted in convictions or guilty pleas of 16 of its members for their role in a global identity theft/cyberfraud scheme. Members of the cybercrime group interacted and communicated primarily through Internet “carding” web sites devoted to trafficking in stolen credit card and personal identifying information and used false identities, anonymous instant messenger accounts, anonymous email accounts, and anonymous virtual currency accounts to conceal the existence and purpose of the criminal enterprise; avoid detection by law enforcement and regulatory agencies; and maintain their anonymity.

The criminal enterprise was composed of vendors, buyers, cybercrime services providers, and money movers located in numerous countries, ranging from Ukraine and throughout Eastern Europe to the United States. The vendors sold nearly 100 000 stolen credit card numbers and other personal identification information through the Internet, taking payment mostly in e-Gold and WebMoney. The buyers used the stolen identities to forge credit cards and purchase expensive merchandise, which they fenced (including via reshipping schemes), committing additional crimes, such as larceny, criminal possession of stolen property, and fraud, and generating about USD 5 million in credit card fraud proceeds. The cybercrime services providers promoted, facilitated, and aided in the purchase, sale and fraudulent use of stolen credit card numbers and other personal identifying information by providing computer services to the vendors and the buyers. The money mover laundered the cybercrime group’s illicit proceeds in a variety of high-tech ways, moving more than USD 35 million through various accounts.

The hub of the entire operation was Western Express International, Inc., a New York corporation based in Manhattan that operated as a virtual currency exchanger and unregistered money transmitter to coordinate and facilitate the Internet payment methods used by the criminal enterprise, and to launder the group’s proceeds. One of the largest virtual currency exchangers in the United States, Western Express International exchanged a total of USD 15 million in WebMoney and USD 20 million in e-Gold for the cybercrime group and used banks and traditional money transmitters to move large sums of money. It also provided information and assistance through its websites (including Dengiforum.com and Paycard2000.com) on ways to move money anonymously and to insulate oneself from reporting requirements.

Western Express International and its owner/operator, a Ukrainian national, plead guilty in February 2013 in New York State to money laundering, fraud, and conspiracy offenses. (In February 2006, Western Express was also indicted for running an illegal check cashing/wire transfer service.) Three other defendants were convicted after trial in June 2013; several more plead guilty in August 2009. Two indicted defendants remain fugitives. The investigation was conducted jointly by the US Secret Service and the Manhattan (New York County) District Attorney’s Office and was successfully prosecuted by the Manhattan District Attorney’s Office.

NOTES

- ¹ The first draft of this paper was prepared jointly by Australia, Canada, Russia, the United Kingdom and the United States for the FATF meetings in February 2014. After that all delegations were invited to provide comments on the draft with a view to adopting a final paper at the next meeting. Comments were received from 10 delegations, and these have been taken into account in preparing this revision.
- ² “Bitcoin” (capitalised) refers to both the open source software used to create the virtual currency and the peer-to-peer (P2P) network formed as a result; “bitcoin” (lowercase) refers to the individual units of the virtual currency.
- ³ It should also be noted that some observers, including former US Federal Reserve Chairman Alan Greenspan, Nout Wellink, a former President of the Dutch Central Bank, and Nobel Laureate economist Robert Shiller, maintain that virtual currency is a passing fad or bubble, akin to Tulipmania in 17th Century Netherlands.
- ⁴ Virtual currency is a complex subject that implicates not only AML/CFT issues, but also other regulatory matters, including consumer protection, prudential safety, tax and soundness regulation, and network IT security standards. The proposed vocabulary is thus relevant across a number of complementary regulatory jurisdictions. Adoption of consistent terms and a common conceptual understanding of virtual currency by all relevant government entities is important to avoid duplicating efforts and/or working at unintended cross purposes, and facilitates the capacity of governmental authorities to leverage their various perspectives and areas of expertise in order to most effectively identify and address relating to virtual currencies.
- ⁵ **Digital representation** is a representation of something in the form of digital data—i.e., computerised data that is represented using discrete (discontinuous) values to embody information, as contrasted with continuous, or analog signals that behave in a continuous manner or represent information using a continuous function. A physical object, such as a flash drive or a bitcoin, may contain a digital representation of virtual currency, but ultimately, the currency only functions as such if it is linked digitally, via the Internet, to the virtual currency system.
- ⁶ Legal tender status does not necessarily require an entity or individual to accept payment in a particular type of legal tender. For example, in many jurisdictions, a private business, person, or organisation is free to develop internal policies on whether or not to accept the jurisdiction’s physical currency or coins (cash) as payment for goods and/or services.
- ⁷ This definition differs from that offered in 2012 by the European Central Bank (ECB), which defined virtual currency “as a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community” ECB, *Virtual Currency Schemes* (October 2012), p. 6. The ECB recognised on p.13 of its report that its “definition may need to be adapted in future if fundamental characteristics change.” Its definition now appears too limited, since math-based, decentralised virtual currencies like Bitcoin are not issued and controlled by a central developer, and some jurisdictions (e.g., the United States, Sweden, and Thailand) now regulate virtual currencies.
- ⁸ This categorisation differs from the ECB’s three-part classification, which divides virtual currencies into three types: “Type 1 . . . refer[s] to closed virtual currency schemes . . . used in an online game. Type 2 . . . [refers to] schemes [that] have a unidirectional flow (usually an inflow), i.e. there is a conversion rate for purchasing the virtual currency, which can . . . be used to buy virtual goods and services . . . (and exceptionally also . . . real goods and services) . . . Type 3 [refers to] schemes . . . [with] bidirectional flows, i.e. the virtual currency . . . acts like any . . . convertible [real] currency, with . . . [buy and sell] exchange rates . . . [and] can . . . be used to buy [both] virtual . . . [and] real goods and services.” ECB *Virtual Currency Schemes*, p. 6. This discussion paper adopts a simpler, bifurcated classification because at present, only (fully) convertible virtual currencies that can be used to move value into and out of the formal financial sector present significant AML/CFT risks. This is because money laundering requires: Conversion or transfer (of illicit funds); concealment or disguise of the source/origin (of illicit funds); or acquisition/possession/use (of illicit funds).
- ⁹ Some convertible virtual currencies can be exchanged directly through the issuing administrator (directly exchanged); others must be exchanged through a virtual currency exchanger (third-party exchanged).

- ¹⁰ For example, WebMoney is a virtual currency because “valuables” (assets) are transferred and stored in the form of a non-fiat currency. The units of measurement of the valuables' property rights stored by the guarantor are WebMoney Title Units (WM) of the corresponding type. <http://wmtransfer.com/eng/about/>
- ¹¹ For example, despite such deterrence measures, several exchanges allow blackmarket conversion of World of Warcraft Gold.
- ¹² A third-party is an individual or entity that is involved in a transaction but is not one of the principals and is not affiliated with the other two participants in the transaction—i.e., a third party functions as a neutral entity between the principals (e.g., sender and receiver, buyer and seller) in a business or financial transaction. The third party's involvement varies with the type of business or financial transaction. For example, an online payment portal, such as PayPal, acts as a third party in a retail transaction. A seller offers a good or service; a buyer uses a credit or debit card entered through the PayPal payment service; and the trusted third party completes the financial transfer. Similarly, in a real estate transaction, a third-party escrow company acts as a neutral agent between the buyer and seller, collecting the documents from the seller and money from the buyer that the two principals need to exchange to complete the transaction.
- ¹³ Distributed is a term of art that refers to an essential feature of decentralised math-based virtual currencies: transactions are validated by a *distributed* proof-of-work system. Each transaction is *distributed* among a network of participants who run the algorithm to validate the transaction.
- ¹⁴ Apart from the initial creation and issuance of ripple coins (RXP), Ripple operates as a decentralised virtual currency. Ripple's founders created all 100 billion ripple coins and retained 20 billion of them, with the remainder to be distributed by a separate entity, Ripple Labs. However, all transactions are verified by a decentralised computer network, using Ripple's open source protocol, and recorded in a shared ledger that is a constantly updated database of Ripple accounts and transactions.
- ¹⁵ In 2140, the block award will cease to be available and miners will be rewarded only by transaction fees.
- ¹⁶ For example, PayPal is actively looking at accepting and clearing bitcoins on the PayPal platform, and JP Morgan Chase has filed a US patent application for an online electronic payments system using a math-based virtual currency protocol that would enable users to make anonymous payments without providing an account number or name, with the virtual currency to be stored on JPMC computers and verified through a shared log, much like the 'block chain' in the bitcoin system.
- ¹⁷ For instance, it remains to be seen whether virtual currency systems can provide a pathway to other financial services, like credit and insurance.
- ¹⁸ The Liberty Reserve investigation and takedown involved law enforcement action in 18 countries and jurisdictions, including Costa Rica; the Netherlands; Spain; Morocco; Sweden; Switzerland; Cyprus; Australia; China; Hong Kong, China; Norway; Latvia; Luxembourg; the United Kingdom; Russia; Canada; and the United States to restrain criminal proceeds, forfeit domain names, and seize servers.
- ¹⁹ The Silk Road investigation involved multiple US law enforcement agencies, led the Federal Bureau of Investigation's (FBI's) New York Special Operations and Cyber Division, and the Drug Enforcement Administration's (DEA's) New York Organized Crime Drug Enforcement Strike Force (comprised of agents and officers of DEA, the Internal Revenue Service (IRS), the New York City Police Department, US Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI), the New York State Police, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the US Secret Service, the US Marshals Service, Office of Foreign Assets Control (OFAC), and NY Department of Taxation), with assistance and support of the ICE-HIS Chicago field office, the Department of Justice's Computer Crime and Intellectual Property and Asset Forfeiture and Money Laundering Sections, the United States Attorney's Office for the Southern District of New York, and foreign law enforcement partners, particularly the Reykjavik Metropolitan Police of the Republic of Iceland and the French Republic's Central Office for the Fight Against Crime Linked to Information Technology and Communication.

BIBLIOGRAPHY AND SOURCES

FATF (2013), *FATF Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services*, FATF, Paris

www.fatf-gafi.org/topics/fatfrecommendations/documents/rba-npps-2013.html

Popper, N. (2013), “In Bitcoin’s Orbit: Rival Virtual Currencies vie for Acceptance”, in *New York Times, Dealbook*, (Nov. 24, 2013) http://dealbook.nytimes.com/2013/11/24/in-bitcoins-orbit-rival-virtual-currencies-vie-for-acceptance/?_r=0, accessed June 2014.

FATF



GUIDANCE FOR A RISK-BASED APPROACH

VIRTUAL CURRENCIES

JUNE 2015

Appendix B



FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

www.fatf-gafi.org

© 2015 FATF/OECD. All rights reserved.

No reproduction or translation of this publication may be made without prior written permission.

Applications for such permission, for all or part of this publication, should be made to the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France

(fax: +33 1 44 30 61 37 or e-mail: contact@fatf-gafi.org).

Photocredits coverphoto: ©Thinkstock

TABLE OF CONTENTS

TABLE OF ACRONYMS	2
SECTION I – INTRODUCTION	3
Background	3
Purpose of the Guidance.....	3
Scope of the Guidance	4
Structure.....	5
SECTION II - SCOPE OF FATF STANDARDS	6
Initial Risk Assessment	6
FATF Definitions	6
SECTION III – APPLICATION OF FATF STANDARDS TO COUNTRIES AND COMPETENT AUTHORITIES	8
SECTION IV – APPLICATION OF FATF STANDARDS TO COVERED ENTITIES.....	12
Potential Solutions to Compliance Challenges.....	14
SECTION V - COUNTRY (OR GROUP OF COUNTRIES) EXAMPLES OF RISK-BASED APPROACH TO VCPPS	15
APPENDIX A VIRTUAL CURRENCIES - KEY DEFINITIONS AND POTENTIAL AML/CFT RISKS	25
Introduction	25
Key Definitions:	26
Legitimate Uses	31
Potential Risks	31
Law Enforcement Actions Involving Virtual Currency.....	32
nOTES	35
Bibliography aND sOURCES.....	38
APPENDIX B HOW DECENTRALISED CONVERTIBLE VIRTUAL CURRENCY WORKS AS A PAYMENTS MECHANISM.....	39
Introduction	39
Scope	39
Participating in the Bitcoin Network to Send and Receive Bitcoins.....	40

TABLE OF ACRONYMS

AML	Anti-money laundering
ATM	Automated teller machine
BaFIN	German Federal Supervisory Authority
CDD	Customer due diligence
CFT	Countering the financing of terrorism
DNFBP	Designated non-financial business and profession
EBA	European Banking Authority
FINMA	Financial Market Supervisory Authority
KWG	German Banking Act
MAS	Monetary Authority of Singapore
ML	Money laundering
MSB	Money service business
MVTS	Money value transfer service
NPPS	New Payment Products and Services
P2P	Peer-to-peer
RBA	Risk-based approach
TF	Terrorist financing
VC	Virtual currency
VCPPS	VC payment products and services

SECTION I – INTRODUCTION

BACKGROUND

1. The Financial Action Task Force (FATF) issued the report [Virtual Currencies Key Definitions and Potential AML/CFT Risks](#), in June 2014 (June 2014 VC report). In recent years, virtual currencies (VCs) have emerged and attracted investment in payments infrastructure built on their software protocols. These payments mechanisms seek to provide a new method for transmitting value over the internet.
2. The FATF recognizes financial innovation. At the same time, VC payment products and services (VCPSS) present money laundering and terrorist financing (ML/TF) risks and other crime risks that must be identified and mitigated. This Guidance focuses on applying the risk based approach to the ML/TF risks associated with VCPSS, and not on other types of VC financial products, such as VC securities or futures products. Accordingly, the Guidance has adopted the term VC payments products and services (VCPSS), rather than VC products and services (VCPS), where the discussion is limited to VC payments schemes.
3. The development of VCPSS and interactions of VCPSS with other New Payment Products and Services (NPPS) and even with traditional banking services,¹ give rise to the need for this Guidance to protect the integrity of the global financial system.
4. This stand-alone Guidance builds on the June 2014 VC report and on the risk matrix and the best practices of the [Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet Based Payment Services](#)² report (June 2013 NPPS report).
5. This Guidance is part of a staged approach taken by the FATF. The focus of this Guidance is on the points of intersection that provide gateways to the regulated financial system, in particular convertible³ virtual currency exchangers⁴. The FATF will continue to monitor developments in VCPSS and emerging risks and mitigating factors. As we learn more about the technology and use of VCPSS, the Guidance may be updated, to include, where appropriate, emerging best practices to address regulatory issues arising in respect of ML/TF risks associated with VCPSS. Issues related to e.g. transfers within decentralised convertible VC networks that do not involve exchange activities, such as person-to-person transfers involving hosted wallet providers, and large value VC payments, which are not addressed by this Guidance may be considered in the longer term.

PURPOSE OF THE GUIDANCE

6. This Guidance is intended to explain the application of the risk-based approach to AML/CFT measures in the VC context; identify the entities involved in VCPSS; and clarify the application of the relevant *FATF Recommendations* to convertible virtual currency exchangers. This Guidance is also intended to help national authorities understand and potentially develop regulatory responses including the need to amend their national laws in order to address the ML/TF risk of VCPSS. This Guidance is also intended to help the private sector better understand the relevant AML/CFT

obligations and how they can effectively comply with relevant requirements. The Guidance incorporates the conceptual framework and key terms adopted by the FATF in the *June 2014 VC Report (Appendix A)*, and readers are referred to that document for discussion of potential use cases for VC and a glossary of terms.

7. The Guidance seeks to:
 - a) Show how specific *FATF Recommendations* should apply to convertible virtual currency exchangers in the context of VCPSS, identify AML/CFT measures that could be required, and provide examples; and
 - b) Identify obstacles to applying mitigating measures rooted in VCPSS's technology and/or business models and in legacy legal frameworks.
8. The FATF notes that some Governments are beginning to consider a range of regulatory issues presented by VCPSS. With respect to AML/CFT in particular, while some jurisdictions are taking regulatory action, others are monitoring and studying the developments and potential ML/TF risks, as the usage still develops in those jurisdictions. For some jurisdictions, putting in place an effective AML/CFT regulatory regime may require a more thorough understanding of the VCPSS. Nevertheless, the rapid development, increasing functionality, growing adoption and global nature of VCPSS make national action to identify and mitigate the ML/TF risks presented by VCPSS a priority. The FATF recognizes that there may be other policy considerations that may affect the ultimate regulatory options or outcomes of VCPSS in individual jurisdictions.
9. Establishing some form of Guidance across all jurisdictions that treat similar products and services consistently according to their function and risk profile is essential to enhance the effectiveness of the international AML/CFT standards. This is a particular concern for VCPSS given their 'borderless' nature, where activities may be carried out without seeming to be based in any particular jurisdiction. While the Guidance is non-binding and does not overrule the purview of national authorities, it hopefully will help public authorities and the private sector identify and effectively address VCPSS associated ML/TF risks.

SCOPE OF THE GUIDANCE

10. The Guidance focuses on VCPSS and related AML/CFT issues, and applies to both centralised and decentralised VCPSS. It primarily addresses convertible VC, because of its higher risks. The focus of this Guidance is on convertible virtual currency exchangers which are points of intersection that provide gateways to the regulated financial system (where convertible VC activities intersect with the regulated fiat currency financial system). It does not address non-AML/CFT regulatory matters implicated by VC payment mechanisms (e.g., consumer protection, prudential safety and soundness, tax, anti-fraud issues and network IT security standards). Nor does it address non-payments uses of VC (e.g., store-of-value products for savings or investment purposes, such as derivatives, commodities, and securities products) or the monetary policy dimension of VC activities.⁵

STRUCTURE

11. This Guidance is organised as follows: Section II examines the extent to which convertible virtual currency exchangers fall within the scope of the *FATF Recommendations*. Section III describes the application of the *FATF Recommendations* to countries and competent authorities; Section IV explains the application of the *FATF Recommendations* to convertible virtual currency exchangers; and Section V provides country (or group of countries) examples of regulatory approaches to date or expected in the near future. The June 2014 VC Report is included in **Appendix A**. An explanation of what VC is and how it works as a payment mechanism, based on different business models and methods of operation, is set forth in **Appendix B**.

SECTION II - SCOPE OF FATF STANDARDS⁶

12. This section (1) discusses the application of the risk-based approach to VCPSS and (2) examines how convertible virtual currency exchangers should be subject to AML/CFT requirements covered by the international standards.

INITIAL RISK ASSESSMENT⁷

13. The risk assessment in the June 2014 VC Report (Appendix A) indicates that at least in the near-term, only *convertible* VC, which can be used to move value into and out of fiat currencies and the regulated financial system, is likely to present ML/TF risks. Accordingly, under the RBA, countries should focus their AML/CFT efforts on higher-risk convertible VCs.

14. The risk assessment also suggests that AML/CFT controls should target convertible VC nodes—i.e., points of intersection that provide gateways to the regulated financial system—and not seek to regulate users who obtain VC to purchase goods or services. These nodes include third-party convertible VC exchangers. Where that is the case, they should be regulated under the *FATF Recommendations*. Thus, countries should consider applying the relevant AML/CFT requirements specified by the international standards to convertible VC exchangers, and any other types of institution that act as nodes where convertible VC activities intersect with the regulated fiat currency financial system.

15. Under the RBA, countries could also consider regulating financial institutions or DNFBP that send, receive, and store VC, but do not provide exchange or cash-in/cash-out services between virtual and fiat currency. This is however, not in the scope of this Guidance.

FATF DEFINITIONS

16. The *FATF Recommendations* require all jurisdictions to impose specified AML/CFT requirements on financial institutions and designated non-financial businesses and professions (DNFBP) and to ensure their compliance with those obligations.

17. The FATF defines a “financial institution” as any natural or legal person who conducts as a business one or more of several specified activities for or on behalf of a customer. The categories potentially most relevant to currently available VCPSS include persons that conduct as a business: Money or value transfer services (MVTSS)⁸; acceptance of deposits and other repayable funds from the public; issuing and managing means of payment; and trading in foreign exchange, or transferable securities. Depending on their particular activities, decentralised VC exchangers, wallet providers, and payments processors/senders, as well as other possible VC business models, may fall within one or more of these categories.

18. Whether a natural or legal person engaged in VCPSS is an obliged entity depends on how that person uses the VC and for whose benefit. National authorities should address the ML/TF risks associated with convertible VC exchange activities (where convertible VC activities intersect with the

regulated fiat currency financial system), as appropriate under their national legal frameworks, which may offer a variety of options for regulating such activity.

19. Providers of VCPSS conducting activities which fall within the FATF definition of a *financial institution* are subject to the applicable FATF Recommendations. This includes convertible virtual currency exchangers where convertible VC activities intersect with the regulated fiat currency financial system.

20. Depending on the intensity or volume of specific VC activities involved and their own national legal frameworks, countries should address the ML/TF risks associated with VC exchanges and any other types of institutions that act as nodes where convertible VC activities intersect with the regulated fiat currency financial system, by applying the relevant FATF Recommendations to any of these categories of covered entities, on a risk basis.

SECTION III – APPLICATION OF FATF STANDARDS TO COUNTRIES AND COMPETENT AUTHORITIES

21. This section explains how specific FATF Recommendations related to VCPSS apply to countries and competent authorities, focusing on identifying and mitigating risks associated with convertible VCs, applying licensing/registration requirements, implementing effective supervision, providing a range of effective and dissuasive sanctions and facilitating national and international cooperation.

22. Some of FATF Recommendations are directly relevant to understanding how countries should use government authorities and international cooperation to address the ML/TF risks associated with convertible VC.

23. **Recommendation 1.** The current *FATF Recommendations* make clear that countries should apply a RBA to ensure that measures to prevent or mitigate ML/TF risks are commensurate with the risks identified. Under the RBA, countries should strengthen the requirements for higher risk situations. When assessing the ML/TF risk of convertible VC, the distinction between centralised and decentralised VC will be one key aspect. Due to anonymity and the challenges to conduct a proper identification of the participant, convertible decentralised VCPSSs in general may be regarded of higher risk of ML/TF which would require the application of enhanced due diligence measures.

24. Recommendation 1 requires countries to identify, understand, and assess the country's ML/TF risks and to take action aimed at effectively mitigating those risks. This requirement applies in relation to risks associated with VCs and other new technologies. Public-private sector cooperation may assist competent authorities in developing AML/CFT policies for VC financial activities, innovations in VC technologies and emerging products and services. This may also assist countries in allocating and prioritizing AML/CFT resources by competent authorities.

25. National authorities should consider undertaking a coordinated risk assessment of VC products and services that (1) enables all relevant authorities to understand how specific VC products and services function, fit into, and impact all relevant regulatory jurisdictions for AML/CFT purposes (e.g., money transmission/payments mechanisms; VC ATMs; commodities; securities) and (2) promotes similar AML/CFT treatment for similar products and services having similar risk profiles.

26. Countries should also require financial institutions and DNFBP to identify, assess, and take effective action to mitigate their ML/TF risks associated with VCPSS. For AML/CFT purposes, where VCPSS activities are permitted under national law, jurisdictions, financial institutions and DNFBP, including convertible virtual currency exchangers, must assess the ML/TF risks and apply a RBA to ensure that appropriate measures to prevent or mitigate those risks are implemented.

27. Even if a country decides not to regulate VC with respect to non-ML/TF risks, such as consumer protection, prudential safety and soundness, and network security, it still should take

prompt action to identify, assess, and apply a RBA to mitigate the ML/TF risks associated with VC under the relevant FATF Recommendations.

28. According to this risk assessment, countries should decide to regulate exchanges platforms between convertible virtual currencies and fiat currencies (i.e., convertible virtual currency exchangers). Some countries may decide to prohibit VC activities, based on their own risk assessment (including, e.g., uptake trends) and national regulatory context in order to support other policy goals not addressed by this Guidance (e.g., consumer protection, safety and soundness, monetary policy). Where countries consider prohibiting VCPs, they should take into account, among other things, the impact a prohibition would have on the local and global level of ML/TF risks, including whether prohibiting VC payments activities could drive them underground, where they will continue to operate without AML/CFT controls or oversight. Regardless of whether a country opts for prohibiting or regulating VCs, additional measures are useful to mitigate the overall ML/TF risk. If a country decides to prohibit VC activities, additional mitigation measures would include identifying VC providers that are operating illegally in their jurisdiction and applying proportionate and dissuasive sanctions to them. Prohibition would still require outreach, education and enforcement actions by the country. Countries would also need to take into account the cross-border element of VCPs in their risk mitigation strategies.

29. **Recommendation 2** requires national cooperation and coordination with respect to AML/CFT policies--including in the VC sector. Countries may consider putting in place mechanisms, such as inter-agency working groups, to enable policy-makers, regulators, supervisors, the financial intelligence unit (FIU), and law enforcement authorities to cooperate with each other and any other relevant competent authorities to develop and implement effective policies, regulations and other measures to address VC ML/TF risks.

30. Countries may consider developing national coordination mechanisms that facilitate appropriate risk-based AML/CFT regulation and supervision across various VC products and services. Among other things, national authorities may undertake a risk assessment of VCPs that (1) enables all relevant authorities to understand how specific VC products and services function, fit into, and impact all relevant regulatory jurisdictions for AML/CFT purposes (e.g., money transmission/payments systems; VC ATMs; commodities; securities) and (2) promotes similar AML/CFT treatment for similar products and services having similar risk profiles. Countries should also consider adopting their national cooperation and coordination mechanism(s) that facilitates engagement with the VC private sector.

31. If VC evolves into a meaningful part of the financial sector, countries should consider examining the relationship of VC AML/CFT regulation and supervision to the non-AML/CFT regulation and supervision of VCs (e.g., consumer protection, safety and soundness, insurance, network security, tax compliance). In this regard, it is recommended that countries should consider undertaking short- and longer-term policy work to develop comprehensive regulation of VCPs if widespread adoption of VC occurs.

32. **Recommendation 14** directs countries to register or license natural or legal persons that provide MVTS in the country, and ensure their compliance with the relevant AML/CFT measures.

This includes subjecting MVTS operating in the country to monitoring for compliance with registration/licensing and other applicable AML/CFT measures.

33. The registration/licensing requirements of Recommendation 14 apply to domestic entities providing convertible VC exchange services between VC and fiat currencies (i.e. VCPSS) in a jurisdiction.

34. Because convertible VC exchangers that transfer value digitally, via the internet, are not subject to territorial boundaries and generally offer VCPSS to persons in countries in which they are not physically present, it is very important that all home countries apply domestic licensing or registration requirements when required by the FATF Recommendations. For the same reasons, proper oversight by the home jurisdiction and adequate cooperation and information exchange between competent authorities between jurisdictions where the entity provides services is of high importance.

35. **Recommendation 15** reinforces the fundamental RBA obligation with respect to new technologies. It requires countries to identify and assess ML/TF risks relating to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Recommendation 15 also requires countries to ensure that financial institutions licensed by or operating in their jurisdiction take appropriate measures to manage and mitigate risk *before* launching new products or business practices or using new or developing technologies. National requirements concerning new technologies should include VCPSS.

36. **Recommendation 16** establishes the requirements for countries with respect to wire transfers. Recommendation 16 applies to cross-border wire transfers and domestic wire transfers. A wire transfer refers to any transaction carried out on behalf of an originator (a) through a financial institution (b) by electronic means with a view to making an amount of funds available to a beneficiary person or (c) at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person. Countries should ensure that when convertible virtual currency exchangers conduct convertible VC transfers that are wire transfers, they include required originator and beneficiary information specified by Recommendation 16. In this regard, countries may adopt a *de minimis* threshold for cross-border wire transfers no higher than USD/EUR 1 000. Countries should also ensure that financial institutions monitor convertible VC transfers to detect those lacking required originator and/or beneficiary information and take appropriate measures to address that situation if it occurs.

37. **Recommendation 26** requires countries to ensure that convertible VC exchangers which act as nodes where convertible VC activities intersect with the regulated fiat currency financial system are subject to adequate regulation and supervision. Countries should consider amending legacy legal frameworks, as needed, to authorize effective AML/CFT regulation of decentralised VC payment mechanisms.

38. **Recommendation 35** directs countries to have a range of effective, proportionate and dissuasive sanctions (criminal, civil or administrative) available to deal with natural or legal persons covered by Recommendations 6 and 8 to 23, that fail to comply with the applicable AML/CFT requirements. However, at present, VCPSS, especially decentralised convertible VCPSS, presents

numerous challenges to applying traditional law enforcement tools and conducting successful prosecutions. The current anonymity of most decentralised VC transactions makes it difficult to determine the identities of the persons involved. The underlying protocols on which almost all decentralised VCPPS are currently based do not require or provide identification and verification of participants. Moreover, the historical transactions records generated on the blockchain by the underlying protocols are not necessarily associated with real world identity. This level of anonymity limits the blockchain's usefulness for monitoring transactions and identifying suspicious activity, and presents a significant challenge to law enforcement's ability to trace illicit proceeds that are laundered using decentralised convertible VC. Furthermore law enforcement cannot target one central location or entity for investigative purposes. These challenges undermine countries' ability to employ effective, dissuasive sanctions. Countries should conduct a review of the challenges that exist in their specific country context to identify potential gaps and take action, as appropriate. Licensing or registration of VC-exchangers, and application of customer identification/verification and recordkeeping requirements, could provide a pathway enabling countries to better apply effective and dissuasive sanctions in the VC context.

39. **Recommendations 40** requires countries to provide efficient and effective international cooperation to help other countries combat ML, associated predicate offences and TF—including mutual legal assistance (**Recommendation 37**); help identifying, freezing, seizing and confiscating proceeds and instrumentalities of crime that may take the form of VC (**Recommendation 38**); and effective extradition assistance in the context of virtual currency related crimes (**Recommendation 39**). These requirements may also apply to cooperation that involves VC. It is also important that the FIUs should cooperate and exchange information on the STRs with their counterparts, especially in relation with cross border operations of VC. Sufficient oversight and regulatory control of convertible VCPPS operating in their jurisdiction enables countries to better provide investigatory assistance and other international cooperation in the VC space. At present, the lack of VC regulation and investigation capacity in most countries may present obstacles to countries' ability to provide meaningful international cooperation. Moreover, many countries do not have legal frameworks that allow them to criminalize certain VC ML/TF activities, which could prevent their providing effective MLA in situations where dual criminality is required.

SECTION IV – APPLICATION OF FATF STANDARDS TO COVERED ENTITIES

40. This section explains how specific *FATF Recommendations* should apply to Convertible VC exchanges and any other type of entities that act as nodes where convertible VC activities intersect with the regulated fiat currency financial system, to mitigate the ML/TF risks associated with VCPSSs. These should include applying a RBA (Recommendation 1), customer due diligence (CDD) (Recommendation 10); record-keeping (Recommendation 11); registration or licensing requirements for MVTS (Recommendation 14) identification and mitigation of risks associated with new technologies (Recommendation 15); AML/CFT program requirements (Recommendation 18) and suspicious transaction reporting (Recommendation 20). This section also examines current obstacles to applying some of these mitigating measures in the decentralised VC space. Recommendation 14 is discussed only in section III above, but as noted requires covered entities to comply with registration or licensing requirement in all jurisdiction where they provide VC MVTS.

41. **Recommendation 1.** The *FATF Recommendations* make clear that countries should require financial institutions and DNFBP to identify, assess, and take effective action to mitigate their ML/TF risks (including those associated with VCPSS). This includes on-going efforts to refine technical processes used to reliably identify and verify customers. For AML/CFT purposes, where VC activities are permitted under national law, all jurisdictions, financial institutions and DNFBPs, including convertible virtual currency exchangers, should assess the ML/TF risks posed by VC activities and apply a RBA to ensure that appropriate measures to prevent or mitigate those risks are implemented. The RBA does not imply the automatic or wholesale denial of services to VCPSS without an adequate risks assessment.

42. **Recommendation 10.** CDD is an essential measure to mitigate the ML/TF risks associated with convertible VC. In accordance with the FATF Standards, countries should require convertible VC exchangers to undertake customer due diligence when establishing business relations or when carrying out (non-wire) occasional transactions using reliable, independent source documents, data or information.⁹ For example, convertible VC exchangers should be required to conduct customer due diligence when exchanging VC for fiat currency or vice versa in a one-off transaction greater than the designated threshold of USD/EUR 15 000 or (b) carrying out occasional transactions that are wire transfers covered by Recommendation 16 and its Interpretive Note. Usually, convertible VC transactions will involve a wire transfer and therefore be subject to Recommendation 16.

43. Countries may wish to consider having a lower or no threshold for VC CDD requirements if appropriate, given the nature and level of identified ML/TF risks.

44. In light of the nature of VCPSS, in which customer relationships are established, funds loaded and transactions transmitted entirely through the internet, institutions must necessarily rely on non-face-to-face identification and verification. Countries should consider requiring entities providing VCPSS to follow the best practices suggested in the *June 2013 NPPS Guidance*. These, to the extent applicable, include: corroborating identity information received from the customer, such as a

national identity number, with information in third party databases or other reliable sources; potentially tracing the customer's Internet Protocol (IP) address; and searching the Web for corroborating activity information consistent with the customer's transaction profile, provided that the data collection is in line with national privacy legislation.

45. Where convertible VCPPS are presenting higher risk, as ascertained on the basis of the RBA, convertible virtual currency exchangers should be required to conduct enhanced CDD in proportion to that risk, and encouraged to use multiple techniques to take reasonable measures to verify customer identity. Where convertible virtual currency exchangers are permitted to complete verification after establishing the business relationship in order not to interrupt the normal conduct of business (in low risk cases), they should be required to complete verification before conducting occasional transactions above the threshold.

46. Countries should also expect financial institutions and DNFBP to consider risks associated with the source of funding convertible VCPPS. Decentralised convertible VCPPS allow anonymous sources of funding, including peer-to-peer (P2P) VC transfers and funding by NPPS that are themselves anonymous, increasing ML/TF risks. As with NPPS, VCPPS business should consider, for occasional transactions above a given threshold, limiting the source of funds to a bank account, credit or debit card, or at least applying such limitations to initial loading, or for a set period until a transaction pattern can be established, or for loading above a given threshold.

47. Transaction monitoring is a key risk mitigant in the convertible VC space because of the difficulty of non-face-to-face identity verification and because it is only recently that decentralised convertible VC technology allows certain risk mitigants that may be available for NPPS to be built into decentralised VCPPS in order to restrict functionality and reduce risk. For instance, multi-signature (multi-sig) technology now enables VCPPS to effectively build in loading total wallet value, and value/velocity transaction limits into decentralised VCPPS. However, current decentralised VC technology does not make it possible to effectively build in geographic limits; limit use to the purchase of certain goods and services; or prevent person-to-person transfers.

48. It is recommended that countries encourage transaction monitoring, commensurate with the risk. The public nature of transaction information available on the blockchain theoretically facilitates transaction monitoring, but as noted in the *June 2014 VC Report* (Appendix A), the lack of real world identity associated with many decentralised VC transactions limits the blockchain's usefulness for monitoring transactions and identifying suspicious activity, presenting serious challenges to effective AML/CFT compliance and supervision.

49. **Recommendation 11, Recommendation 20 and Recommendation 22. Recordkeeping and Suspicious activity reporting** when VC transactions could involve the proceeds of criminal activity or be related to terrorist financing, in accordance with Recommendation 20, are also essential. At a minimum, financial institutions and DNFBP should be required to maintain transaction records that include: information to identify the parties; the public keys, addresses or accounts involved; the nature and date of the transaction, and the amount transferred. The public information available on the blockchain provides a beginning foundation for record keeping, provided institutions can adequately identify their customers. Countries should require institutions to be attentive to the type of suspicious activity they are in a position to detect.

50. **Recommendation 15 and Recommendation 22** specifically addresses new technologies and requires financial institutions and DNFBP to identify and assess ML/TF risks relating to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Recommendation 15 also requires financial institutions and DNFBP licensed by or operating in a jurisdiction to take appropriate measures to manage and mitigate risk *before* launching new products or business practices or using new or developing technologies. These measures apply in relation to VC as a new technology. National authorities are expected to enforce this obligation, and financial institutions and DNFBP should be proactive in fulfilling the expectations set forth in Recommendation 15.

POTENTIAL SOLUTIONS TO COMPLIANCE CHALLENGES

51. Financial institutions and DNFBP should be required to comply with customer identification and verification and transaction monitoring requirements for decentralised convertible VCPs, using the most effective and efficient means available, as soon as such products/services are offered. Given the compliance and law enforcement challenges presented by decentralised convertible VC, financial institutions, DNFBP, developers, investors, and other actors in the VC space should seek to develop technology-based solutions that will improve compliance.

52. For example, developers may be able to create new VC technologies, such as application programming interfaces (APIs) that provide customer identification information, or allow financial institutions or DNFBP to limit transaction size and velocity or establish a variety of conditions that must be satisfied before a VC transaction can be sent to the recipient/beneficiary to reduce the ML/TF risks associated with a particular VCP. The possibility of using information collected online to augment the customer profile and help in detecting suspicious activity and transactions is another important AML/CFT compliance growth area. Innovation relevant to AML/CFT compliance may take the form of improving existing VC protocols or developing entirely new VCs, built on fundamentally different underlying protocols that can build-in risk mitigants or facilitate customer identification and transaction monitoring.

53. Third-party digital identity systems may also be developed to facilitate AML/CFT compliance that might better fit VCPs. These systems could, for instance, involve third-party digital identity custodians and/or other entities' creating, authenticating, and maintaining digital identity solutions for specific CDD, monitoring, and reporting purposes, in response to requirements imposed by national AML/CFT laws implementing the international standards. Third party digital identity custodians would themselves need to be regulated to ensure identification/verification integrity.

54. Financial institutions and DNFBP could also explore developing business models to facilitate customer identification/verification, transaction monitoring, and compliance with other relevant AML/CFT requirements. For example, institutions involved in transmitting decentralised convertible VC could consider creating an industry association(s) composed of vetted VC institutions and develop policies and practices for members that allow them to identify specific transactions as coming from a member that has applied appropriate CDD and is conducting appropriate transaction monitoring.

SECTION V - COUNTRY (OR GROUP OF COUNTRIES) EXAMPLES OF RISK-BASED APPROACH TO VCPPS

55. This section gives an overview of the regulatory approaches some countries (or group of countries) have adopted so far as well as the expected approaches by countries in the near future. As mentioned in the introduction, governments around the world are beginning to grapple with the broad range of regulatory challenges presented by VCPPS. A report by the Bank for International Settlements categorizes the measures taken to date as follows.¹⁰

- a) Imposing restrictions on regulated entities for dealing with virtual currencies;
- b) Adopting legislative/regulatory measures, such as the need for exchange platforms dealing with VC to be subject to regulation as money remitters, or the proposed regulation of VC intermediaries in some jurisdictions for AML/CFT purposes;
- c) Publishing statements cautioning users about risks associated with VC and/or clarifying the position of authorities with respect to VC; and
- d) Monitoring and studying developments.

56. The current or contemplated AML/CFT regulatory approaches to VC adopted in a number of jurisdictions as outlined below provide examples of the RBA:

CANADA

57. In June 2014, Canada amended its AML/CFT legislation to treat persons and entities engaged in the business of dealing in VCs as money services businesses (MSBs). Supporting regulations are still under development to define exactly which entities will be covered and their respective obligations. However, it is expected that the obligations will be largely similar to existing MSB obligations, which include registration, CDD (including beneficial ownership information), record keeping and an internal compliance regime, as well as reporting suspicious and certain prescribed transactions.

58. In developing its VC AML/CFT policy, Canada is taking a RBA, including understanding the risks associated with VC in the context of the ML/TF risks faced by Canada, as part of Canada's ML/TF National Risk Assessment. The regulations will balance the needs of mitigating the ML/TF risk with those of fostering continued financial innovation. Therefore, Canada is proposing a targeted regulatory intervention into areas with the greatest ML/TF vulnerabilities.

CHINA

59. On 3rd December of 2013, the People's Bank of China, jointly with the MIIT (Ministry of Industry and Information Technology), the Banking Regulatory Commission (CBRC), the Insurance Regulatory Commission (CIRC) and the Securities Regulatory Commission (CSRC), issued *the Notice on Preventing Risks of Bitcoin*. This notice required institutions which provide services including bitcoin registration, bitcoin wallet and bitcoin exchanging shall fulfill AML/CFT obligations and take

measures to identify its customers and record identification information. Financial institutions and payment services providers were also required to take enhanced monitoring measures on bitcoin service providers to prevent relevant risks. Furthermore, PBC branch offices around the country were required to study bitcoin related ML risks and take commensurate actions including enhanced supervisory actions and enhanced monitoring on suspicious transactions to mitigate risks.

EBA'S OPINION ON "VIRTUAL CURRENCIES"

60. On the 4th July 2014, the European Banking Authority (EBA) issued an Opinion on "virtual currencies", following an analysis of the risks that these new products could present as long as there are not regulated. The EBA opinion is addressed to EU legislators as well as national supervisory authorities in the 28 Member States.

61. The EBA Opinion is built around long term and short term recommendations aiming at establishing a comprehensive regulatory approach.

62. From the EBA perspective, a potential long term regulatory approach would require a substantial body of regulation and would need to comprise, amongst other elements, governance requirements for several market participants, the segregation of client accounts, capital requirements, and the creation of "scheme governing authorities" that are accountable for the integrity of a virtual currencies scheme and its key components, including its protocol and transaction ledger.

63. However, as long as no such regime is in place, the EBA opinion considers that some of the more pressing risks identified will need to be mitigated in other ways. As an "immediate response", the EBA advises national authorities to make financial institutions aware of the risks of, and discourage them from buying, holding or selling virtual currencies. The EBA also recommends that EU legislators consider declaring virtual currency exchanges as 'obliged entities' that must comply with anti-money laundering and counter terrorist financing requirements set out in the EU Anti Money Laundering Directive. Commission negotiations on the 4th Anti-money laundering Directive did not adopt the EBA's July 2014 recommendation. Instead, the Commission will assess options for more comprehensive regulation over the medium term. Its upcoming supranational AML/CFT risk assessment will include an assessment of the risks posed by VC and make appropriate recommendations to Member States.

FRANCE

64. On 29 January 2014, the French Prudential Supervisory and Resolution Authority (ACPR) issued a position statement, emphasizing that an entity engaged in intermediation with respect to the purchase or sale of VC in exchange for fiat currency is a financial intermediary who receives funds on a third party's behalf, and that these activities must be authorised by the ACPR and are therefore subject to AML/CFT requirements. In June 2014, the French FIU, TRACFIN, published a report, "Regulating Virtual Currencies: Recommendations to prevent virtual currencies from being used for fraudulent purposes and money laundering," intended to establish a framework to deter the use of virtual currencies for fraud and money laundering.

GERMANY

65. The German Federal Supervisory Authority (BaFin) qualifies Bitcoin with legally binding effect as financial instruments in the form of units of account in accordance with section 1 (11) sentence 1 of the German Banking Act (KWG). These units are comparable to currencies, but are not denominated legal tender.

66. Bitcoin are not e-money within the meaning of the German Payment Services Supervision Act (ZAG), because no Bitcoin are issued representing a receivable from an issuer. This is different for virtual currencies, which are backed by a central issuer. Bitcoin are not legal tender either, and therefore qualify as neither currency nor banknotes and coins.

67. Commercial activities related to financial instruments generally do require a license from BaFin. But BaFin has also clarified that the use of Bitcoin as a substitute currency for trade payments itself is not an activity subject to authorisation under the KWG. Mining of Bitcoin per se is not an activity subject to authorisation either, because miners do not issue or place any Bitcoin themselves. The same applies to the purchase or sale of mined or acquired Bitcoin, which does not require authorisation either.

68. However, an authorisation requirement may arise if there are additional factors. Often Bitcoin are traded via internet platforms, some of which are referred to as exchanges. Such activities generally do require authorisation by BaFin. Which authorisation is required can only be determined by analysing the technical and contractual implementation of the transactions in detail. Some may carry on investment broking as defined in the KWG, others may operate a multilateral trading facility, which is a financial service specified in the KWG. There are some, that might be regarded as principal broking services. If potential buyers and sellers are merely introduced to each other on platforms, this does not constitute the brokering of specific transactions. In such cases, however, the providers on these types of platforms are proprietary traders subject to an authorisation requirement within the meaning of the KWG. Providers acting as exchange bureaus that offer to change legal currencies directly into Bitcoin also meet the criterion of proprietary trading subject to an authorisation requirement.

69. Since each case is different, mining pools, i.e. the pooling of computer processing power in general by several persons for the purpose of jointly generating Bitcoin, are not necessarily subject to supervision. As a general rule, if several persons use processing power with equal rights and subsequently distribute the Bitcoin proportionately, this is not an activity that requires authorisation. Different rules may apply if the pool operator commercially offers a share of the revenue from mined or sold Bitcoin against the provision of processing power and the participants have no control over the specific processes, for example.

70. BaFin receives a growing number of enquiries on derivative and fund-like products related to Bitcoin. Again, since each case is different, they are not necessarily subject to supervision. In general, however, if traded commercially, these types of products are subject to the supervisory rules of the KWG or the KAGB, because products derived from a financial instrument are themselves financial instruments or at least represent asset management. The commercial operation of a bitcoin ATM is normally also a banking or financial service subject to an authorisation requirement – depending on

the way the purchase processes and legal relationships are arranged between buyer, seller and – in some cases – operator.

71. BaFin assumes that a business is carried on in Germany not only if the service provider's registered office or habitual residence is in Germany, but also if it is located abroad and the service provider targets the market to repeatedly and commercially offer banking or financial services to companies or persons whose registered office or habitual residence is in Germany. However, this does not affect the passive freedom to provide services, i.e. the right of persons and companies resident in Germany to request services from a foreign provider under their own initiative. Transactions that have been entered into because the customer has taken the initiative do not, therefore, require authorisation under the KWG. For online offerings relating to financial market products, the relevant criterion is whether analysis of the website as a whole reveals that the services offered are targeted at the German market. A disclaimer is only one of many indicators. Other indications include the domain and top-level domain, the language or other country-specific references and the legal framework.

72. Banks and financial services providers already holding an authorisation to trade in financial instruments are also permitted to engage in transactions with Bitcoin without being subject to any further authorisation requirements. In all these cases the authorised institution is also an obliged entity under AML-legislation.

HONG KONG, CHINA

73. Hong Kong, China has taken a very cautious approach since mid-2013 in reminding the public of the consumer, money laundering and cyber crime risks associated with any trading or dealing in virtual currencies and virtual commodities, such as Bitcoin. Hong Kong, China does not regulate such virtual commodities per se, as they are not “currency”, “securities” or “legal tender” in existing legislation. Likewise, operators or dealers providing services in relation to virtual commodities do not fall within the definition of a “money service business” under the Anti-Money Laundering and Counter Terrorist Financing (Financial Institutions) Ordinance, unless their services or transactions involve money changing or remittance services. That said, financial institutions, virtual commodity dealers or operators, or individuals are subject to a statutory duty to report suspicious transactions to the Joint Financial Intelligence Unit, if their due diligence work or transactions reveal any suspicious activities in relation to money laundering or terrorist financing, regardless of whether virtual commodities are involved. A failure to disclose such suspicious transactions may amount to a criminal offence. Existing laws also cover acts of fraud, technology crimes, pyramid scheme, money laundering or terrorist financing involving virtual commodities. In addition, regulators have issued guidance to financial institutions to remind them to ensure an escalated level of vigilance commensurate with money laundering and terrorist financing risks associated with virtual commodities. Financial institutions have been reminded to exercise caution in assessing relevant money laundering or terrorist financing risks when establishing or maintaining business relationships with customers and clients who are operators of any schemes or businesses relating to virtual commodities.

ITALY

74. In Italy virtual currencies are not considered legal tender. In January 2015, Bank of Italy issued a warning on the use of so-called virtual currencies¹¹ and a communication, included in Supervisory Bulletin n.1, 2015, which endorses the EBA “Opinion on ‘virtual currencies’”; the latter discourages banks and other supervised financial intermediaries from buying, holding or selling virtual currencies. In the same date, the Italian Financial Intelligence Unit issued a communication on the anomalous use of virtual currencies and on the detection of suspicious money laundering or terrorist financing transactions by obliged entities¹².

RUSSIA

75. Pursuant to Article 27 of Federal law “On the Central Bank of the Russian Federation (Bank of Russia)”, issuing monetary surrogates is prohibited in the Russian Federation. In January 2014 the Central Bank of the Russian Federation released “Information on virtual currencies, particularly Bitcoin, used for conducting transactions” on its official website. The Bank of Russia warns individuals, legal entities and, primarily, credit institutions and non-credit financial institutions, against the use of virtual currencies in exchange for goods, services or real currency in rubles or foreign currency. Due to the anonymous nature of the issue of virtual currencies by an unlimited number of persons and use of such currencies for conducting transactions, individuals and legal entities may unwittingly become involved in illegal activities, including ML/FT. Therefore, exchanging virtual currencies for real currency in rubles or foreign currency, as well as for goods and services, will be viewed by the Bank of Russia as potential involvement of a legal entity in conducting suspicious transactions specified in the current AML/CFT legislation.

76. With the view to mitigating ML/FT risks associated with virtual currencies, the Ministry of Finance, jointly with the Bank of Russia, developed the draft law imposing a ban on electronic monetary surrogates and electronic monetary surrogates transactions. The Draft has been prepared and will be introduced into the Parliament (State Duma).

SINGAPORE

77. In March 2014, the Monetary Authority of Singapore (MAS) announced it will regulate VC intermediaries operating in Singapore to address potential ML/TF risks. The MAS will introduce regulations requiring VC intermediaries that buy, sell or facilitate the exchange of VCs for fiat currencies to verify customer identity and report suspicious transactions. The proposed regulations do not address the safety and soundness of VC intermediaries, nor the proper functioning of VC transactions.

78. The proposed regulatory framework for virtual currency intermediaries has not been implemented yet. The current intention is to only regulate virtual currency intermediaries that operate in Singapore; i.e. those which have a physical presence in the country. However, as the virtual currency space is evolving rapidly, Singapore will continue to closely monitor the regulatory approaches taken towards virtual currencies by other jurisdictions. If necessary, MAS will consider additional measures to address the risks posed by virtual currencies and their intermediaries.

SOUTH AFRICA

79. The National Treasury issued a user alert to the monitoring of virtual currency on 18 September 2014.¹³ This was a combined statement between the National Treasury, the South African Reserve Bank, the Financial Services Board, the South African Revenue Service and the Financial Intelligence Centre to warn members of the public to be aware of the risks associated with the use of virtual currencies for either transactions or investments.

80. Currently in South Africa there are no specific laws or regulations that address the use of virtual currencies. Consequently, no legal protection or recourse is afforded to users of virtual currencies. Due to their unregulated status in South Africa, virtual currencies cannot be classified as legal tender as any merchant may refuse them as a payment instrument without being in breach of the law. Virtual currencies also cannot be regarded as a means of payment as they are not issued on receipt of funds. Dealing in virtual currencies is, therefore, performed at the user's own risk with no recourse to the South African authorities. The South African authorities will continue to monitor and assess the use of virtual currencies and consult with private sector stakeholders in this regard. Further guidance or regulations may be issued, should the need arise.

SWITZERLAND

81. In June 2014, the Swiss Government published a study and policy statement on VC, the *Federal Council Report on Virtual Currencies in Response to the Schwaab (13.3687) and Weibel (13.4070) Postulates*,¹⁴ which declared that "Professional trade in virtual currencies and the operation of trading platforms in Switzerland generally come under the scope of the *Anti-Money Laundering Act*." Entities engaged in these activities are required to comply "with the obligation to verify the identity of the contracting party and establish the identity of the beneficial owner." At the same time, Swiss Financial Market Supervisory Authority (FINMA) published a fact sheet,¹⁵ emphasizing that the purchase and sale of convertible VC on a commercial basis and the operation of trading platforms used to transfer money or convertible VC from a platform's users to other users are subject to Switzerland's Anti-Money Laundering Act. Before commencing operations, a provider of these kinds of services must either become a member of a self-regulatory organisation (SRO) or apply to FINMA for a license to operate as a directly supervised financial intermediary (DSFI). Where decentralised VC trading activities fall under the Anti-Money Laundering Act, compliance with CDD obligations is mandatory. Because convertible VC can facilitate anonymity and cross-border asset transfers, FINMA considers trading in it to have heightened ML/TF risks, requiring strict CDD, particularly as regards client identification. Commercial activities involving convertible VC require a banking license when an organisation, as part of its business activities, accepts convertible VC from clients and administer VC holdings for clients. VC entities that obtain banking licenses are subject to prudential supervision by FINMA, which will monitor the company on an ongoing basis to ensure that it complies with the relevant regulations. The Federal Council is continuing to monitor developments in the area of VCs to identify any need for additional action at an early stage.

UNITED KINGDOM

82. UK Government's plans for virtual currencies: in November 2014, the UK Government published a Call for Information to gather evidence on the benefits and risks associated with virtual (digital) currencies, with a particular focus on the question of regulation. The Call for Information closed in December 2014. In March 2015, the UK Government published a summary of the evidence gathered through the Call for Information, and announced that it intends to apply anti-money laundering regulation to digital currency exchanges in the UK. The UK Government plans to formally consult on the detail of the proposed regulatory approach later this year.

83. UK's efforts to improve its understanding of the risks with regards virtual currencies: The level of understanding of the risk around VC in the UK has improved. The UK's National Crime Agency (NCA) is leading a multi-agency response to evaluating and responding to the threat posed by the criminal use of VCs, involving the Crown Prosecution Service, HM Revenue & Customs, City of London Police, HM Treasury, Bank of England, Financial Conduct Authority, Home Office and the Metropolitan Police Service.

84. This work includes building the intelligence picture. An NCA assessment has provided a baseline for law enforcement on the threat posed by the criminal use of VCs. An improved intelligence picture will be the basis for operational targeting, and is also being fed into policy makers to inform decision making about government intervention. Capacity building work includes awareness raising with industry and Forces. In addition, much of this activity is being mirrored at the international level, which is important given the cross border nature of the problem.

UNITED STATES

85. The United States regulates any natural and legal person—including convertible VC exchangers and administrators—engaged in the acceptance and transmission of convertible VC from one person to another person or location as money transmitters, subject to AML/CFT obligations, including registration, customer identification, record-keeping and reporting requirements. The federal AML/CFT regulation covers both centralised and decentralised convertible VCs and applies to persons engaged in transmitting convertible VC on behalf of a third person without also exchanging VC back-and-forth for fiat currency. It also applies to foreign-located convertible VC exchangers/administrators that have no physical presence in the United States, but that do business in whole or substantial part within the United States. Current U.S. Government AML/CFT regulations do not apply to users of convertible VC who are using the VC without engaging in money transmission. In addition to federal regulations, 48 states regulate money transmitters, and many are considering how their legacy AML/CFT and prudential regulation of money transmitters may apply to VCs. For example, the New York Financial Services Department (NYFSD) has announced that it will shortly issue a regulation requiring some virtual currency businesses to obtain "bitlicenses" and comply with AML/CFT obligations, consumer disclosure rules, capital requirements, and investment rules.

86. The U.S. undertook legal changes in order to accommodate changing financial technology. Recognizing that AML/CFT protections must keep pace with the emergence of new payment systems, in July 2011, FinCEN amended its rule dealing with Money Services Businesses (MSBs)

generally¹⁶, providing the flexibility needed to accommodate VC payments innovations under the existing Bank Secrecy Act (BSA) regulatory framework. The amended MSB added the phrase, “other value that substitutes for currency” to the definition of “money transmission services” and thereby changed the definition of money transmitter MSBs. As a result of this regulatory change, “money transmission services” is now defined as “the acceptance of currency, funds, *or other value that substitutes for currency* from one person *and* the transmission of currency, funds, *or other value that substitutes for currency* to another location or person by any means.”¹⁷ A “money transmitter” is a person (individual or entity) that provides money transmission services or any other person engaged in the transfer of funds. Since “money transmission services,” is defined as “the acceptance of currency, funds, *or other value that substitutes for currency* from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means,” the United States is able to regulate any legal or natural person engaged in accepting convertible VC from one person and transmitting it to another person or location, thus covering, among others, convertible virtual currency exchangers and administrators as money transmitters.

NOTES

- ¹ For example, a U.S.-based Bitcoin wallet provider/exchanger/payments processor, links the customer's VC wallet to a bank account or traditional charge or debit card for funding VC purchases and receiving VC cash-out. A UK-based Bitcoin remittance service in the UK-Kenya corridor links to a Kenyan mobile payments system at the delivery end. A Bitcoin exchange operating in Europe recently added branded network credit and debit cards to its available funding options, which already included Single Euro Payments Area (SEPA) bank **transfers**. A Bitcoin exchange headquartered in Australia, with customers in over 40 countries, sends remittances directly to the beneficiary's bank account without the recipient using Bitcoin, but with the backend of the remittance conducted entirely in bitcoins.
- ² FATF (2013), *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet Based Payment Services*, FATF, Paris, France, www.fatf-gafi.org/topics/fatfrecommendations/documents/rba-npps-2013.html
- ³ **Convertible** means that the virtual currency can be exchanged for fiat currency.
- ⁴ A **virtual currency exchanger** is a person or entity engaged as a business in the exchange of virtual currency for real currency, funds, or other forms of virtual currency and also precious metals, and vice versa, for a fee (commission). Exchangers generally accept a wide range of payments, including cash, wires, credit cards, and other virtual currencies, and can be administrator-affiliated, non-affiliated, or a third party provider. Exchangers can act as a bourse or as an exchange desk. Individuals typically use exchangers to deposit and withdraw money from virtual currency accounts.
- ⁵ Since VC can function as a medium of exchange, unit of account, and/or store of value, it may raise issues across a number of complementary regulatory jurisdictions, including, e.g., commodities and securities regulation.
- ⁶ The FATF Standards comprise the FATF Recommendations and their Interpretive Notes.
- ⁷ *Virtual Currencies Key Definitions and Potential AML/CFT Risks* (FATF, 2014).
- ⁸ The FATF defines MVTs as financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTs provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and **may include any new payment methods...** [emphasis added].
- ⁹ For the complete list of activities covered by the definition of "financial institutions," see the *FATF Recommendations Glossary*.
- ¹⁰ Non-Banks in retail payments, Committee on Payments and Market Infrastructures, Bank for International Settlements (September 2014)
- ¹¹ www.bancaditalia.it/compiti/vigilanza/avvisi-pub/index.html
- ¹² http://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/Comunicazione_UIF_su_VV.pdf
- ¹³ National Treasury (2014), *Monitoring of virtual currencies*, National Treasury, Republic of South Africa, available from www.treasury.gov.za/comm_media/press/2014
- ¹⁴ Available at www.news.admin.ch/NSBSubscriber/message/attachments/35355.pdf

¹⁵ Available at www.finma.ch/e/finma/publikationen/faktenblaetter/Documents/fb-bitcoins-e.pdf

¹⁶ The *Bank Secrecy Act Regulations – Definitions and Other Regulations Relating to Money Services Businesses*, 76 FR 43585 (July 21, 2011), 31 CFR § 1010.100(ff)(5)(i)(A) (the MSB Rule). At almost the same time, FinCEN also issued a new Final Rule dealing with prepaid access (*Final Rule – Definitions and Other Regulations Relating to Prepaid Access*, 76 FR 45403 (July 29, 2011), 31 CFR § 1010.100(ww)(5)(i)(A) (the Prepaid Access Rule)).

¹⁷ 31 CFR § 1010.100(ff)(5)(i)(A) (emphasis added).

APPENDIX A

VIRTUAL CURRENCIES - KEY DEFINITIONS AND POTENTIAL AML/CFT RISKS¹

Appendix A was originally published by the FATF as a stand-alone paper in June 2014

INTRODUCTION

As decentralised, math-based virtual currencies—particularly Bitcoin²—have garnered increasing attention, two popular narratives have emerged: (1) virtual currencies are the wave of the future for payment systems; and (2) virtual currencies provide a powerful new tool for criminals, terrorist financiers and other sanctions evaders to move and store illicit funds, out of the reach of law enforcement and other authorities.³ Against this backdrop, this paper builds on the 2013 New Payment Products and Services (NPPS) Guidance (FATF, 2013) by suggesting a conceptual framework for understanding and addressing the anti-money laundering / countering the financing of terrorism (AML/CFT) risks associated with one kind of internet-based payment system: virtual currencies. Specifically, the paper proposes a common definitional vocabulary that clarifies what virtual currency is and classifies the various types of virtual currency, based on their different business models and methods of operation,⁴ and identifies the participants in typical virtual currency systems. It also applies risk factors set forth in Section IV (A) of the 2013 NPPS Guidance to specific types of virtual currencies to identify potential risks; describes some recent investigations and enforcement efforts involving virtual currency; and presents a sample of jurisdictions' current regulatory approaches to virtual currency.

While the 2013 NPPS Guidance broadly addressed internet-based payment services, it did not define “digital currency,” “virtual currency,” or “electronic money.” Nor did it focus on virtual currencies, as distinct from internet-based payment systems that facilitate transactions denominated in real money (fiat or national currency) (e.g., Pay-Pal, Alipay, or Google Checkout). It also did not address decentralised convertible virtual currencies, such as Bitcoin. The 2013 Guidance also notes that, “[g]iven the developing nature of alternate online currencies, the FATF may consider further work in this area in the future” (2013 NPPS Guidance, p. 11, para. 29). A short-term typologies project on this basis was initiated with the following objectives:

- develop a risk-matrix for virtual currencies (or perhaps, more broadly, for both virtual currencies and e-money);
- promote fuller understanding of the parties involved in convertible virtual currency systems and the way virtual currency can be used to operate payment systems; and
- stimulate a discussion on implementing risk-based AML/CFT regulations in this area.

This typologies project may lead to policy work by the FATF, e.g. the issuance of supplemental guidance for applying a risk-based approach to virtual currencies that would incorporate the proposed vocabulary and risk-matrix developed by the typologies project and explain how specific FATF Recommendations apply in the context of virtual currency.

KEY DEFINITIONS:

A common set of terms reflecting how virtual currencies operate is a crucial first step to enable government officials, law enforcement, and private sector entities to analyse the potential AML/CFT risks of virtual currency as a new payment method. As regulators and law enforcement officials around the world begin to grapple with the challenges presented by virtual currencies, it has become apparent that we lack a common vocabulary that accurately reflects the different forms virtual currency may take. The following set of terms is intended to aid discussion between FATF members. It is important to note that this vocabulary may change as virtual currency evolves and as regulators and law enforcement/government officials continue to consider the challenges virtual currencies present. Nevertheless, the proposed vocabulary aims to provide a common language for developing conceptual tools to help us better understand how virtual currencies operate and the risks and potential benefits they offer.

VIRTUAL CURRENCY

Virtual currency is a digital representation⁵ of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment)⁶ in any jurisdiction.⁷ It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency. Virtual currency is distinguished from **fiat currency** (a.k.a. “**real currency**,” “**real money**,” or “**national currency**”), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from **e-money**, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency—i.e., it electronically transfers value that has legal tender status.

Digital currency can mean a digital representation of either virtual currency (non-fiat) or e-money (fiat) and thus is often used interchangeably with the term “virtual currency”. In this paper to avoid confusion, only the terms “virtual currency” or “e-money” are used.

CONVERTIBLE VERSUS NON-CONVERTIBLE VIRTUAL CURRENCY

This paper proposes dividing virtual currency into two basic types: convertible and non-convertible virtual currency.⁸ Although the paper uses “non-convertible” and “closed”, and “convertible” and “open” as synonyms, it should be emphasised that the notion of “convertible currency” does not in any way imply an ex officio convertibility (e.g. in the case of gold standard), but rather a de facto convertibility (e.g. because a market exists). Thus, a virtual currency is “convertible” only as long as

some private participants make offers and others accept them, since the “convertibility” is not guaranteed at all by law.

Convertible (or open) virtual currency has an equivalent value in real currency and can be exchanged back-and-forth for real currency.⁹ Examples include: Bitcoin; e-Gold (defunct); Liberty Reserve (defunct); Second Life Linden Dollars; and WebMoney.¹⁰

Non-convertible (or closed) virtual currency is intended to be specific to a particular virtual domain or world, such as a Massively Multiplayer Online Role-Playing Game (MMORPG) or Amazon.com, and under the rules governing its use, cannot be exchanged for fiat currency. Examples include: Project Entropia Dollars; Q Coins; and World of Warcraft Gold.

It should be noted that even where, under the terms set by the administrator, a non-convertible currency is officially transferrable only within a specific virtual environment and is not convertible, it is possible that an unofficial, secondary black market may arise that provides an opportunity to exchange the “non-convertible” virtual currency for fiat currency or another virtual currency. Generally, the administrator will apply sanctions (including termination of membership and/or forfeiture of remaining virtual currency) to those seeking to create or use a secondary market, contrary to the rules of the currency.¹¹ Development of a robust secondary black market in a particular “non-convertible” virtual currency may, as a practical matter, effectively transform it into a convertible virtual currency. A non-convertible characterisation is thus not necessarily static.

CENTRALISED VERSUS NON-CENTRALISED VIRTUAL CURRENCIES

All non-convertible virtual currencies are centralised: by definition, they are issued by a central authority that establishes rules making them non-convertible. In contrast, convertible virtual currencies may be either of two sub-types: centralised or decentralised.

Centralised Virtual Currencies have a single administrating authority (**administrator**)—i.e., a third party¹² 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). The exchange rate for a convertible virtual currency may be either **floating**—i.e., determined by market supply and demand for the virtual currency--or **pegged**—i.e., fixed by the administrator at a set value measured in fiat currency or another real-world store of value, such as gold or a basket of currencies. Currently, the vast majority of virtual currency payments transactions involve centralised virtual currencies. Examples: E-gold (defunct); Liberty Reserve dollars/euros (defunct); Second Life “Linden dollars”; PerfectMoney; WebMoney “WM units”; and World of Warcraft gold.

Decentralised Virtual Currencies (a.k.a. crypto-currencies) are distributed¹³, open-source, math-based peer-to-peer virtual currencies that have no central administrating authority, and no central monitoring or oversight. Examples: Bitcoin; Litecoin; and Ripple.¹⁴

Cryptocurrency refers to a math-based, decentralised convertible virtual currency that is protected by cryptography.—i.e., it incorporates principles of cryptography to implement a distributed, decentralised, secure information economy. Cryptocurrency relies on public and private keys to transfer value from one person (individual or entity) to another, and must be cryptographically

signed each time it is transferred. The safety, integrity and balance of cryptocurrency [ledgers](#) is ensured by a network of mutually distrustful parties (in Bitcoin, referred to as miners) who protect the network in exchange for the opportunity to obtain a randomly distributed fee (in Bitcoin, a small number of newly created bitcoins, called the “block reward” and in some cases, also transaction fees paid by users as a incentive for miners to include their transactions in the next block). Hundreds of cryptocurrency specifications have been defined, mostly [derived from](#) Bitcoin, which uses a proof-of-work system to validate transactions and maintain the block chain. While Bitcoin provided the first fully implemented cryptocurrency protocol, there is growing interest in developing alternative, potentially more efficient proof methods, such as systems based on proof-of-stake.

Bitcoin, launched in 2009, was the first decentralised convertible virtual currency, and the first cryptocurrency. Bitcoins are units of account composed of unique strings of numbers and letters that constitute units of the currency and have value only because individual users are willing to pay for them. Bitcoins are digitally traded between users with a high degree of anonymity and can be exchanged (purchased or cashed out) into US dollars, Euros, and other fiat or virtual currencies. Anyone can download the free, open-source software from a website to send, receive, and store bitcoins and monitor Bitcoin transactions. Users can also obtain Bitcoin addresses, which function like accounts, at a Bitcoin exchanger or online wallet service. Transactions (fund flows) are publicly available in a shared transaction register and identified by the Bitcoin address, a string of letters and numbers that is not systematically linked to an individual.. Therefore, Bitcoin is said to be “pseudo-anonymous”. Bitcoin is capped at 21 million bitcoins (but each unit could be divided in smaller parts), projected to be reached by 2140.¹⁵ As of April 2, 2014, there were over 12-and-a-half million bitcoins, with total value of slightly more than USD 5.5 billion, based on the average exchange rate on that date.

Altcoin refers to math-based decentralised convertible virtual currency other than bitcoins, the original such currency. Current examples include Ripple; PeerCoin, Lite-coin; zerocoin; anoncoin and dogecoin. One popular exchanger, Cryptsy, would reportedly exchange over 100 different virtual currencies (as of 2 April 2014). (Popper, N., 2013)

Anonymiser (anonymising tool) refers to tools and services, such as darknets and mixers, designed to obscure the source of a Bitcoin transaction and facilitate anonymity. (Examples: Tor (darknet); Dark Wallet (darknet); Bitcoin Laundry (mixer)).

Mixer (laundry service, tumbler) is a type of anonymiser that obscures the chain of transactions on the blockchain by linking all transactions in the same bitcoin address and sending them together in a way that makes them look as if they were sent from another address. A mixer or tumbler sends transactions through a complex, semi-random series of dummy transactions that makes it extremely difficult to link specific virtual coins (addresses) with a particular transaction. Mixer services operate by receiving instructions from a user to send funds to a particular bitcoin address. The mixing service then “comingles” this transaction with other user transactions, such that it becomes unclear to whom the user intended the funds to be directed. (Examples: Bitmixer.io; SharedCoin; Blockchain.info; Bitcoin Laundry; Bitlaunder; Easycoin).

Tor (originally, The Onion Router) is an underground distributed network of computers on the Internet that conceals the true IP addresses, and therefore the identities of the network’s users, by

routing communications/transactions through multiple computers around the world and wrapping them in numerous layers of encryption. Tor makes it very difficult to physically locate computers hosting or accessing websites on the network. This difficulty can be exacerbated by use of additional tumblers or anonymisers on the Tor network. Tor is one of several underground distributed computer networks, often referred to as darknets, cypherspace, the Deep web, or anonymous networks, which individuals use to access content in a manner designed to obscure their identity and associated Internet activity.

Dark Wallet is a browser-based extension wallet, currently available on Chrome (and potentially on Firefox), that seeks to ensure the anonymity of Bitcoin transactions by incorporating the following features: auto-anonymiser (mixer); decentralised trading; uncensorable crowd funding platforms; stock platforms and information black markets; and decentralised market places similar to Silk Road.

Cold Storage refers to an offline Bitcoin wallet—i.e., a Bitcoin wallet that is not connected to the Internet. Cold storage is intended to help protect the stored virtual currency against hacking and theft.

Hot Storage refers to an online bitcoin wallet. Because it is connected to the Internet, hot storage is more vulnerable to hacking/theft than cold storage.

Local Exchange Trading System (LETS) is a locally organised economic organisation that allows members to exchange goods and services with others in the group. LETS use a locally created currency to denominate units of value that can be traded or bartered in exchange for goods or services. Theoretically, bitcoins could be adopted as the local currency used within a LETS. (Examples: Ithica Dollars; Mazacoin).

VIRTUAL CURRENCY SYSTEM PARTICIPANTS

An **exchanger (also sometimes called a virtual currency exchange)** is a person or entity engaged as a business in the exchange of virtual currency for real currency, funds, or other forms of virtual currency and also precious metals, and vice versa, for a fee (commission). Exchangers generally accept a wide range of payments, including cash, wires, credit cards, and other virtual currencies, and can be administrator-affiliated, non-affiliated, or a third party provider. Exchangers can act as a bourse or as an exchange desk. Individuals typically use exchangers to deposit and withdraw money from virtual currency accounts.

An **administrator** is a person or entity engaged as a business in **issuing** (putting into circulation) a centralised virtual currency, establishing the rules for its use; maintaining a central payment ledger; and who has the authority to **redeem** (withdraw from circulation) the virtual currency.

A **user** is a person/entity who obtains virtual currency and uses it to purchase real or virtual goods or services or send transfers in a personal capacity to another person (for personal use), or who holds the virtual currency as a (personal) investment. Users can obtain virtual currency in several ways. For example, they can (1) purchase virtual currency, using real money (from an exchanger or, for certain centralised virtual currencies, directly from the administrator/issuer); (2) engage in specific activities that earn virtual currency payments (e.g., respond to a promotion, complete an

online survey, provide a real or virtual good or service); (3) with some decentralised virtual currencies (e.g., Bitcoin), self-generate units of the currency by "mining" them (see definition of miner, below), and receive them as gifts, rewards, or as part of a free initial distribution.

A **miner** is an individual or entity that participates in a decentralised virtual currency network by running special software to solve complex algorithms in a distributed proof-of-work or other distributed proof system used to validate transactions in the virtual currency system. Miners may be users, if they self-generate a convertible virtual currency solely for their own purposes, e.g., to hold for investment or to use to pay an existing obligation or to purchase goods and services. Miners may also participate in a virtual currency system as exchangers, creating the virtual currency as a business in order to sell it for fiat currency or other virtual currency.

Virtual currency wallet is a means (software application or other mechanism/medium) for holding, storing and transferring bitcoins or other virtual currency.

A **wallet provider** is an entity that provides a virtual currency wallet (i.e., a means (software application or other mechanism/medium) for holding, storing and transferring bitcoins or other virtual currency). A wallet holds the user's private keys, which allow the user to spend virtual currency allocated to the virtual currency address in the block chain. A wallet provider facilitates participation in a virtual currency system by allowing users, exchangers, and merchants to more easily conduct the virtual currency transactions. The wallet provider maintains the customer's virtual currency balance and generally also provides storage and transaction security. For example, beyond providing bitcoin addresses, the wallet may offer encryption; multiple key (multi-key) signature protection, backup/cold storage; and mixers. All Bitcoin wallets can interoperate with each other. Wallets can be stored both online ("hot storage") or offline ("cold storage"). (Examples: Coinbase; Multibit; Bitcoin Wallet).

In addition, various **other entities** may participate in a virtual currency system and may be affiliated with or independent of exchangers and/or administrators. These include **web administration service providers (a.k.a. web administrators)**; **third party payments senders** facilitating merchant acceptance; **software developers**; and **application providers** (some of the "other entities" listed in this paragraph may already fall into one of the categories above.). Applications and software development can be for legitimate purposes—e.g., to increase ease of merchant acceptance and customer payments or to respond to legitimate privacy concerns—or for illicit purposes—e.g., a mixer developer/operator can target illicit users with products designed to avoid regulatory and law enforcement scrutiny.

It must be emphasised that this list of participants is not exhaustive. Moreover, given the rapid development of virtual currency technologies and business models, additional participants could arise within virtual currency systems and pose potential AML/CFT risks.

Taxonomy of Virtual Currencies

	Centralised	Decentralised
Convertible	Administrator, exchangers, users; third-party ledger; can be exchanged for fiat currency. Example: WebMoney	Exchangers, users (no administrator); no Trusted Third-Party ledger; can be exchanged for fiat currency. Example: Bitcoin
Non-convertible	Administrator, exchangers, users; third-party ledger; cannot be exchanged for fiat currency. Example: World of Warcraft Gold	Does not exist

LEGITIMATE USES

Like other new payment methods, virtual currency has legitimate uses, with prominent venture capital firms investing in virtual currency start-ups. Virtual currency has the potential to improve payment efficiency and reduce transaction costs for payments and fund transfers. For example, Bitcoin functions as a global currency that can avoid exchange fees, is currently processed with lower fees/charges than traditional credit and debit cards, and may potentially provide benefit to existing online payment systems, like Paypal.¹⁶ Virtual currency may also facilitate micro-payments, allowing businesses to monetise very low-cost goods or services sold on the Internet, such as one-time game or music downloads. At present, as a practical matter, such items cannot be sold at an appropriately low per/unit cost because of the higher transaction costs associated with e.g., traditional credit and debit. Virtual currency may also facilitate international remittances and support financial inclusion in other ways, as new virtual currency-based products and services are developed that may potentially serve the under- and un-banked. Virtual currency - notably, Bitcoin - may also be held for investment. These potential benefits need to be carefully analysed, including whether claimed cost advantages will remain if virtual currency becomes subject to regulatory requirements similar to those that apply to other payments methods, and/or if exchange fees for cashing out into fiat currency are factored in, and whether volatility, consumer protection and other factors¹⁷ limit their potential for financial inclusion.

POTENTIAL RISKS

Convertible virtual currencies that can be exchanged for real money or other virtual currencies are potentially vulnerable to money laundering and terrorist financing abuse for many of the reasons identified in the 2013 NPPS Guidance. First, they may allow greater anonymity than traditional non-cash payment methods. Virtual currency systems can be traded on the Internet, are generally characterised by non-face-to-face customer relationships, and may permit anonymous funding (cash funding or third-party funding through virtual exchangers that do not properly identify the funding

source). They may also permit anonymous transfers, if sender and recipient are not adequately identified.

Decentralised systems are particularly vulnerable to anonymity risks. For example, by design, Bitcoin addresses, which function as accounts, have no names or other customer identification attached, and the system has no central server or service provider. The Bitcoin protocol does not require or provide identification and verification of participants or generate historical records of transactions that are necessarily associated with real world identity. There is no central oversight body, and no AML software currently available to monitor and identify suspicious transaction patterns. Law enforcement cannot target one central location or entity (administrator) for investigative or asset seizure purposes (although authorities can target individual exchangers for client information that the exchanger may collect). It thus offers a level of potential anonymity impossible with traditional credit and debit cards or older online payment systems, such as PayPal.

Virtual currency's global reach likewise increases its potential AML/CFT risks. Virtual currency systems can be accessed via the Internet (including via mobile phones) and can be used to make cross-border payments and funds transfers. In addition, virtual currencies commonly rely on complex infrastructures that involve several entities, often spread across several countries, to transfer funds or execute payments. This segmentation of services means that responsibility for AML/CFT compliance and supervision/enforcement may be unclear. Moreover, customer and transaction records may be held by different entities, often in different jurisdictions, making it more difficult for law enforcement and regulators to access them. This problem is exacerbated by the rapidly evolving nature of decentralised virtual currency technology and business models, including the changing number and types/roles of participants providing services in virtual currency payments systems. And importantly, components of a virtual currency system may be located in jurisdictions that do not have adequate AML/CFT controls. Centralised virtual currency systems could be complicit in money laundering and could deliberately seek out jurisdictions with weak AML/CFT regimes. Decentralised convertible virtual currencies allowing anonymous person-to-person transactions may seem to exist in a digital universe entirely outside the reach of any particular country.

LAW ENFORCEMENT ACTIONS INVOLVING VIRTUAL CURRENCY

Law enforcement is already seeing cases that involve the abuse of virtual currency for money laundering purposes. Examples include:

LIBERTY RESERVE

In what is to date the largest online money-laundering case in history, in May 2013, the US Department of Justice charged Liberty Reserve, a Costa Rica-based money transmitter, and seven of its principals and employees with operating an unregistered money transmitter business and money laundering for facilitating the movement of more than 6 billion USD in illicit proceeds. In a coordinated action, the Department of the Treasury identified Liberty Reserve as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act, effectively cutting it off from the US financial system.

Established in 2006, Liberty Reserve was designed to avoid regulatory and law enforcement scrutiny and help criminals distribute, store, and launder the proceeds of credit card fraud, identity theft, investment fraud, computer hacking, narcotics trafficking, and child pornography by enabling them to conduct anonymous and untraceable financial transactions. Operating on an enormous scale, it had more than a million users worldwide, including more than 200 000 in the United States, and handled approximately 55 million transactions, almost all of which were illegal. It had its own virtual currency, Liberty Dollars (LR), but at each end, transfers were denominated and stored in fiat currency (US dollars).

To use LR currency, a user opened an account through the Liberty Reserve website. While Liberty Reserve ostensibly required basic identifying information, it did not validate identities. Users routinely established accounts under false names, including blatantly criminal names (“Russia Hackers,” “Hacker Account,” “Joe Bogus”) and blatantly false addresses (“123 Fake Main Street, Completely Made Up City, New York”). To add a further layer of anonymity, Liberty Reserve required users to make deposits and withdrawals through recommended third-party exchangers—generally, unlicensed money transmitting businesses operating in Russia, and in several countries without significant governmental money laundering oversight or regulation at that time, such as Malaysia, Nigeria, and Vietnam. By avoiding direct deposits and withdrawals from users, Liberty Reserve evaded collecting information about them through banking transactions or other activity that would create a central paper trail. Once an account was established, a user could conduct transactions with other Liberty Reserve users by transferring LR from his or her account to other users, including front company “merchants” that accepted LR as payment. For an extra “privacy fee” (75 US cents per transaction), users could hide their Liberty Reserve account numbers when transferring funds, making the transfers completely untraceable. After learning it was being investigated by US law enforcement, Liberty Reserve pretended to shut down in Costa Rica but continued to operate through a set of shell companies, moving millions through their accounts in Australia, Cyprus, China, Hong Kong, Morocco, Russia, Spain and elsewhere.¹⁸

SILK ROAD

In September 2013, the US Department of Justice unsealed a criminal complaint charging the alleged owner and operator of Silk Road, a hidden website designed to enable its users to buy and sell illegal drugs, weapons, stolen identity information and other unlawful goods and services anonymously and beyond the reach of law enforcement, with narcotics trafficking, computer hacking, and money laundering conspiracies. The Justice Department also seized the website and approximately 173 991 bitcoins, worth more than USD 33.6 million at the time of the seizure, from seized computer hardware. The individual was arrested in San Francisco in October and indicted in February 2014; the investigation is ongoing.

Launched in January 2011, Silk Road operated as a global black-market cyber bazaar that brokered anonymous criminal transactions and was used by several thousand drug dealers and other unlawful vendors to distribute unlawful goods and services to over a hundred thousand buyers, a third of whom are believed to have been in the United States. It allegedly generated total sales revenue of approximately USD 1.2 billion (more than 9.5 million bitcoins) and approximately USD 80 million (more than 600 000 bitcoins) in commissions for Silk Road. Hundreds of millions of

dollars were laundered from these illegal transactions (based on bitcoin value as of dates of seizure). Commissions ranged from 8 to 15 percent of total sales price.

Silk Road achieved anonymity by operating on the hidden Tor network and accepting only bitcoins for payment. Using bitcoins as the exclusive currency on Silk Road allowed purchasers and sellers to further conceal their identity, since senders and recipients of peer-to-peer (P2P) bitcoin transactions are identified only by the anonymous bitcoin address/account. Moreover, users can obtain an unlimited number of bitcoin addresses and use a different one for each transaction, further obscuring the trail of illicit proceeds. Users can also employ additional “anonymisers,” beyond the tumbler service built into Silk Road transactions (see discussion below).

Silk Road’s payment system functioned as an internal Bitcoin bank, where every Silk Road user had to hold an account in order to conduct transactions on the site. Every Silk Road user had at least one Silk Road Bitcoin address (and potentially thousands) associated with the user’s Silk Road account, stored on wallets maintained on servers controlled by Silk Road. To make a purchase, a user obtained bitcoins (typically through a Bitcoin exchanger) and sent them to a Bitcoin address associated with his or her Silk Road account to fund the account. When a purchase was made, Silk Road transferred the user’s bitcoins to an escrow account it maintained, pending completion of the transaction, and then transferred the user’s / buyer’s bitcoins from the escrow account to the vendor’s Silk Road Bitcoin address. As a further step, Silk Road employed a “tumbler” for every purchase, which, as the site explained, “sen[t] all payments through a complex, semi-random series of dummy transactions ... --making it nearly impossible to link your payment with any [bit]coins leaving the site.”¹⁹

WESTERN EXPRESS INTERNATIONAL

An eight-year investigation of a multinational, Internet-based cybercrime group, the Western Express Cybercrime Group, resulted in convictions or guilty pleas of 16 of its members for their role in a global identity theft/cyberfraud scheme. Members of the cybercrime group interacted and communicated primarily through Internet “carding” web sites devoted to trafficking in stolen credit card and personal identifying information and used false identities, anonymous instant messenger accounts, anonymous email accounts, and anonymous virtual currency accounts to conceal the existence and purpose of the criminal enterprise; avoid detection by law enforcement and regulatory agencies; and maintain their anonymity.

The criminal enterprise was composed of vendors, buyers, cybercrime services providers, and money movers located in numerous countries, ranging from Ukraine and throughout Eastern Europe to the United States. The vendors sold nearly 100 000 stolen credit card numbers and other personal identification information through the Internet, taking payment mostly in e-Gold and WebMoney. The buyers used the stolen identities to forge credit cards and purchase expensive merchandise, which they fenced (including via reshipping schemes), committing additional crimes, such as larceny, criminal possession of stolen property, and fraud, and generating about USD 5 million in credit card fraud proceeds. The cybercrime services providers promoted, facilitated, and aided in the purchase, sale and fraudulent use of stolen credit card numbers and other personal identifying information by providing computer services to the vendors and the

buyers. The money mover laundered the cybercrime group's illicit proceeds in a variety of high-tech ways, moving more than USD 35 million through various accounts.

The hub of the entire operation was Western Express International, Inc., a New York corporation based in Manhattan that operated as a virtual currency exchanger and unregistered money transmitter to coordinate and facilitate the Internet payment methods used by the criminal enterprise, and to launder the group's proceeds. One of the largest virtual currency exchangers in the United States, Western Express International exchanged a total of USD 15 million in WebMoney and USD 20 million in e-Gold for the cybercrime group and used banks and traditional money transmitters to move large sums of money. It also provided information and assistance through its websites (including Dengiforum.com and Paycard2000.com) on ways to move money anonymously and to insulate oneself from reporting requirements.

Western Express International and its owner/operator, a Ukrainian national, plead guilty in February 2013 in New York State to money laundering, fraud, and conspiracy offenses. (In February 2006, Western Express was also indicted for running an illegal check cashing/wire transfer service.) Three other defendants were convicted after trial in June 2013; several more plead guilty in August 2009. Two indicted defendants remain fugitives. The investigation was conducted jointly by the US Secret Service and the Manhattan (New York County) District Attorney's Office and was successfully prosecuted by the Manhattan District Attorney's Office.

NOTES

- ¹ The first draft of this paper was prepared jointly by Australia, Canada, Russia, the United Kingdom and the United States for the FATF meetings in February 2014. After that all delegations were invited to provide comments on the draft with a view to adopting a final paper at the next meeting. Comments were received from 10 delegations, and these have been taken into account in preparing this revision.
- ² "Bitcoin" (capitalised) refers to both the open source software used to create the virtual currency and the peer-to-peer (P2P) network formed as a result; "bitcoin" (lowercase) refers to the individual units of the virtual currency.
- ³ It should also be noted that some observers, including former US Federal Reserve Chairman Alan Greenspan, Nout Wellink, a former President of the Dutch Central Bank, and Nobel Laureate economist Robert Shiller, maintain that virtual currency is a passing fad or bubble, akin to Tulipmania in 17th Century Netherlands.
- ⁴ Virtual currency is a complex subject that implicates not only AML/CFT issues, but also other regulatory matters, including consumer protection, prudential safety, tax and soundness regulation, and network IT security standards. The proposed vocabulary is thus relevant across a number of complementary regulatory jurisdictions. Adoption of consistent terms and a common conceptual understanding of virtual currency by all relevant government entities is important to avoid duplicating efforts and/or working at unintended cross purposes, and facilitates the capacity of governmental authorities to leverage their various perspectives and areas of expertise in order to most effectively identify and address relating to virtual currencies.

-
- 5 **Digital representation** is a representation of something in the form of digital data—i.e., computerised data that is represented using discrete (discontinuous) values to embody information, as contrasted with continuous, or analog signals that behave in a continuous manner or represent information using a continuous function. A physical object, such as a flash drive or a bitcoin, may contain a digital representation of virtual currency, but ultimately, the currency only functions as such if it is linked digitally, via the Internet, to the virtual currency system.
- 6 Legal tender status does not necessarily require an entity or individual to accept payment in a particular type of legal tender. For example, in many jurisdictions, a private business, person, or organisation is free to develop internal policies on whether or not to accept the jurisdiction’s physical currency or coins (cash) as payment for goods and/or services.
- 7 This definition differs from that offered in 2012 by the European Central Bank (ECB), which defined virtual currency “as a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community” ECB, *Virtual Currency Schemes* (October 2012), p. 6. The ECB recognised on p.13 of its report that its “definition may need to be adapted in future if fundamental characteristics change.” Its definition now appears too limited, since math-based, decentralised virtual currencies like Bitcoin are not issued and controlled by a central developer, and some jurisdictions (e.g., the United States, Sweden, and Thailand) now regulate virtual currencies.
- 8 This categorisation differs from the ECB’s three-part classification, which divides virtual currencies into three types: “Type 1 . . . refer[s] to closed virtual currency schemes . . . used in an online game. Type 2 . . . [refers to] schemes [that] have a unidirectional flow (usually an inflow), i.e. there is a conversion rate for purchasing the virtual currency, which can . . . be used to buy virtual goods and services . . . (and exceptionally also . . . real goods and services) . . . Type 3 [refers to] schemes . . . [with] bidirectional flows, i.e. the virtual currency . . . acts like any . . . convertible [real] currency, with . . . [buy and sell] exchange rates . . . [and] can . . . be used to buy [both] virtual . . . [and] real goods and services.” ECB *Virtual Currency Schemes*, p. 6. This discussion paper adopts a simpler, bifurcated classification because at present, only (fully) convertible virtual currencies that can be used to move value into and out of the formal financial sector present significant AML/CFT risks. This is because money laundering requires: Conversion or transfer (of illicit funds); concealment or disguise of the source/origin (of illicit funds); or acquisition/possession/use (of illicit funds).
- 9 Some convertible virtual currencies can be exchanged directly through the issuing administrator (directly exchanged); others must be exchanged through a virtual currency exchanger (third-party exchanged).
- 10 For example, WebMoney is a virtual currency because “valuables” (assets) are transferred and stored in the form of a non-fiat currency, The units of measurement of the valuables’ property rights stored by the guarantor are WebMoney Title Units (WM) of the corresponding type. <http://wmtransfer.com/eng/about/>
- 11 For example, despite such deterrence measures, several exchanges allow blackmarket conversion of World of Warcraft Gold.
- 12 A third-party is an individual or entity that is involved in a transaction but is not one of the principals and is not affiliated with the other two participants in the transaction—i.e., a third party functions as a neutral entity between the principals (e.g., sender and receiver, buyer and seller) in a business or financial transaction. The third party’s involvement varies with the type of business or financial transaction. For example, an online payment portal, such as PayPal, acts as a third party in a retail transaction. A seller offers a good or service; a buyer uses a credit or debit card entered through the PayPal payment service; and the trusted third party completes the financial transfer. Similarly, in a real

estate transaction, a third-party escrow company acts as a neutral agent between the buyer and seller, collecting the documents from the seller and money from the buyer that the two principals need to exchange to complete the transaction.

- 13 Distributed is a term of art that refers to an essential feature of decentralised math-based virtual currencies: transactions are validated by a *distributed* proof-of-work system. Each transaction is *distributed* among a network of participants who run the algorithm to validate the transaction.
- 14 Apart from the initial creation and issuance of ripple coins (RXP), Ripple operates as a decentralised virtual currency. Ripple's founders created all 100 billion ripple coins and retained 20 billion of them, with the remainder to be distributed by a separate entity, Ripple Labs. However, all transactions are verified by a decentralised computer network, using Ripple's open source protocol, and recorded in a shared ledger that is a constantly updated database of Ripple accounts and transactions.
- 15 In 2140, the block award will cease to be available and miners will be rewarded only by transaction fees.
- 16 For example, PayPal is actively looking at accepting and clearing bitcoins on the PayPal platform, and JP Morgan Chase has filed a US patent application for an online electronic payments system using a math-based virtual currency protocol that would enable users to make anonymous payments without providing an account number or name, with the virtual currency to be stored on JPMC computers and verified through a shared log, much like the 'block chain' in the bitcoin system.
- 17 For instance, it remains to be seen whether virtual currency systems can provide a pathway to other financial services, like credit and insurance.
- 18 The Liberty Reserve investigation and takedown involved law enforcement action in 18 countries and jurisdictions, including Costa Rica; the Netherlands; Spain; Morocco; Sweden; Switzerland; Cyprus; Australia; China; Hong Kong, China; Norway; Latvia; Luxembourg; the United Kingdom; Russia; Canada; and the United States to restrain criminal proceeds, forfeit domain names, and seize servers.
- 19 The Silk Road investigation involved multiple US law enforcement agencies, led the Federal Bureau of Investigation's (FBI's) New York Special Operations and Cyber Division, and the Drug Enforcement Administration's (DEA's) New York Organized Crime Drug Enforcement Strike Force (comprised of agents and officers of DEA, the Internal Revenue Service (IRS), the New York City Police Department, US Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI), the New York State Police, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the US Secret Service, the US Marshals Service, Office of Foreign Assets Control (OFAC), and NY Department of Taxation), with assistance and support of the ICE-HIS Chicago field office, the Department of Justice's Computer Crime and Intellectual Property and Asset Forfeiture and Money Laundering Sections, the United States Attorney's Office for the Southern District of New York, and foreign law enforcement partners, particularly the Reykjavik Metropolitan Police of the Republic of Iceland and the French Republic's Central Office for the Fight Against Crime Linked to Information Technology and Communication.

BIBLIOGRAPHY AND SOURCES

FATF (2013), *FATF Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services*, FATF, Paris

www.fatf-gafi.org/topics/fatfrecommendations/documents/rba-npps-2013.html

Popper, N. (2013), "In Bitcoin's Orbit: Rival Virtual Currencies vie for Acceptance", in *New York Times, Dealbook*, (Nov. 24, 2013) http://dealbook.nytimes.com/2013/11/24/in-bitcoins-orbit-rival-virtual-currencies-vie-for-acceptance/?_r=0, accessed June 2014.

APPENDIX B

HOW DECENTRALISED CONVERTIBLE VIRTUAL CURRENCY WORKS AS A PAYMENTS MECHANISM

INTRODUCTION

1. Bitcoin and other decentralised convertible virtual currencies (VCs) provide potentially ground-breaking alternative digital payments platforms. The Bitcoin network itself was explicitly designed to serve as an electronic **peer-to-peer (P2P)**¹ payments mechanism for Internet-based commerce. It was intended to enable users to bypass financial institutions by directly transferring VC to each other and settling those transactions in near real time, thereby removing intermediation costs, such as transaction fees and payment uncertainty.

2. **Decentralised VC (also commonly referred to as cryptocurrency)**² is distributed, open-source, math-based convertible VC that does not involve a “trusted third party” to verify transactions and maintain (and reconcile) a transaction ledger. Bitcoin provided the first fully implemented cryptocurrency protocol, creating the world’s first decentralised VC payments mechanism. Subsequently, hundreds of cryptocurrency specifications have been defined, mostly derived from Bitcoin, although there is ongoing interest in developing alternative, potentially more efficient protocols, using different proof methods³ to validate transactions and maintain the online distributed transaction ledger.

SCOPE

3. This appendix provides a brief explanation of how decentralised convertible⁴ (VC) operates as a payments mechanism. It focuses on the functional aspects of decentralised convertible VC networks, rather than on technical aspects of the protocol(s), and addresses **single-currency VC payments networks**, like Bitcoin, rather than **currency-agnostic platforms** like Ripple.⁵ The document (1) explains the conceptual framework for decentralised VC and describes the basic components of a single-currency decentralised VC payments network; (2) explains step-by-step what users must do to participate in the Bitcoin network and conduct a transaction; and (3) identifies many of the third-party VC payments products and services (VCPSS) that have recently emerged to facilitate use of this new payments mechanism. The discussion uses Bitcoin to illustrate single-currency decentralised convertible VC payments mechanisms, because of Bitcoin’s first-mover advantage and much greater scale (in terms of transaction number and value and market capitalisation), compared to other decentralised VCs, and because to date, the venture capital investments and developing infrastructure for single-currency decentralised VC payments networks are overwhelmingly Bitcoin-specific. Using a concrete example, in the form of Bitcoin, is important for descriptive clarity; it does not reflect any endorsement by the FATF, nor prediction of eventual success as a mainstream payments mechanism. Many of the terms used in this document are defined in the FATF’s June 2014 *Virtual Currencies—Key Definitions and Potential AML/CFT Risks (June 2014*

VC Document), provided in **Appendix A**. Those that are not are presented in bold and explained herein.

DECENTRALISED VIRTUAL CURRENCY AS A PAYMENTS PLATFORM

CONCEPTUAL FRAMEWORK FOR DECENTRALISED VC PAYMENTS MECHANISMS

4. Disintermediating financial institutions in electronic payments involves a major conceptual step. The Bitcoin protocol was designed to replicate various trust functions that financial institutions typically perform as intermediaries in electronic and cash transactions. One crucial trust function is guaranteeing against “double-spending” and counterfeiting.⁶ **Double-spending** refers to a VC user’s ceding ownership of the VC to one person and then ceding ownership of the same VC to another person. The double-spending problem arises because decentralised VC exists in the form of a digital file that can be easily duplicated and has no trusted authority maintaining a central record of transactions.

5. To prevent double-spending and counterfeiting, Bitcoin relies on a distributed online public ledger, called the **blockchain**,⁷ and on public key cryptography to verify transactions. **Public-key cryptography** is a cryptographic method that assigns a user two keys: a **public key and a private key**. A **public key (a.k.a. Bitcoin address)** is a unique identifier that functions similarly to an e-mail address for the receipt of e-mail, and serves as an account for receiving bitcoins. A **private key** is a cryptographic code that functions as a secret password that allows the user to sign a VC transaction and transfer the bitcoins to another address. Using the private key proves ownership of the bitcoins. Every Bitcoin public key/address has a matching private key. The private key is mathematically related to the Bitcoin address and is designed so that the Bitcoin address can be calculated from the private key, but the same cannot be done in reverse, thus providing transaction and account security. The public key must be paired with the private key (signature) in order for the VC to be transmitted.

6. The Bitcoin protocol requires every transaction to be validated, logged and disclosed⁸ on the blockchain. The **blockchain** functions as a public transaction reporting system. It consists of **blocks**; each block is a grouping of reported transactions in chronological order. When a transaction is initiated (proposed), it is broadcast to the network and participants, called miners, running a special piece of software, validate the transaction by solving a complex mathematical problem that verifies that the bitcoins in the proposed transaction have not already been spent and add it to the blockchain.⁹ This same distributed (community) validation process, called “**mining**,”¹⁰ generates new bitcoins, which are rewarded as payment to the first miner that solves the algorithm validating the transaction.¹¹ Every transaction that ever took place is recorded in order on the blockchain.

PARTICIPATING IN THE BITCOIN NETWORK TO SEND AND RECEIVE BITCOINS

7. Originally, the Bitcoin network was only a P2P transfer system, with no third party products and services. Users obtained and stored bitcoins, and conducted transactions, themselves. As discussed below, Bitcoin payments infrastructure has rapidly evolved, and now offers a variety of third-party payment products and services to facilitate obtaining, storing and using bitcoins. The following section describes the basic components and steps required to participate in the Bitcoin

network and conduct Bitcoin payments transactions. The final section describes some of the entities offering third-party bitcoin products and services.

PARTICIPATION WITHOUT INTERMEDIARIES

Step One: Obtain the Public Keys (Addresses), Private Keys, and Wallets Needed to Participate in the Bitcoin Network

8. At its most basic, to participate in the Bitcoin network *without any intermediaries*, users download and install free Bitcoin software (called the Bitcoin “client”) to their computers from an affiliated website. The client software contains a wallet program that generates and stores public-private key pairs. The public key generated by the software is identified as a unique Bitcoin address (a 24 to 37-character string of numbers and letters), which functions as an account to receive Bitcoin payments and allow a user to conduct Bitcoin transactions. Users can create/obtain as many addresses as they want. The private keys (with Bitcoin, random sequences of 64 letters and numbers) generated by and stored in the client are mathematically linked to a specific Bitcoin address. As a practical matter, private keys **are** the user’s virtual currency. The wallet program also communicates with other Bitcoin addresses on the Bitcoin network, allowing the user to send and receive bitcoins. The user accesses his/her bitcoin through a wallet (a computer file) on his/her computer, mobile phone, or other digital device. Alternatively, users can download a software wallet program from an online third-party wallet provider. Some software wallets operate in coordination with the Bitcoin client, while others allow the user to avoid downloading the entire Bitcoin client itself. A wallet the user downloads and stores on his/her own computer or other digital device is called an **unhosted wallet**. The user can store his/her unhosted wallet online (“hot storage”) or offline (“cold storage”). With unhosted wallets, the owner is responsible for providing wallet security and protecting the private keys.

Step Two: Obtain Bitcoins

9. Users may obtain bitcoins in several ways. For example, they can (1) purchase VC from a third-party exchanger, using fiat money or other VCs; (2) engage in specific activities that earn VC payments (e.g., respond to a promotion, complete an online survey, provide a real or virtual good or service); (3) receive them as gifts or rewards; and (4) self-generate bitcoins by mining¹² them, as described above. The bulk of mining is now concentrated in professionalized mining pools; users typically obtaining bitcoins from third-party exchanges.

Step Three: Transfer Bitcoins

10. Bitcoin transactions are sent from and to Bitcoin addresses in Bitcoin wallets and are digitally signed for security. To use bitcoins to send a payment for goods or services or a remittance—i.e., to spend or send bitcoins—the user uses the private key(s) to unlock his/her digital wallet and digitally sign the transaction. The transaction itself contains three pieces of information: (1) an input (the bitcoin address that was used *to send the bitcoins to the current sender*); (2) an amount (the amount of bitcoins the sender is transferring); and (3) an output (the recipient’s bitcoin address). These automated functions are handled by the wallet software. The user (via the downloaded software)

sends the bitcoins from his/her wallet to the Bitcoin network. At that point, as described above, Bitcoin miners include it in a transaction block, verify the transaction and enter it onto the blockchain, confirming the transaction. Most Bitcoin transactions that are conducted by the user him/herself, without intermediaries, have no mandatory fees. However, it is now recommended that users pay a voluntary fee to remunerate the miners for faster confirmation.

Figure 1. The three essential elements of a Bitcoin transaction

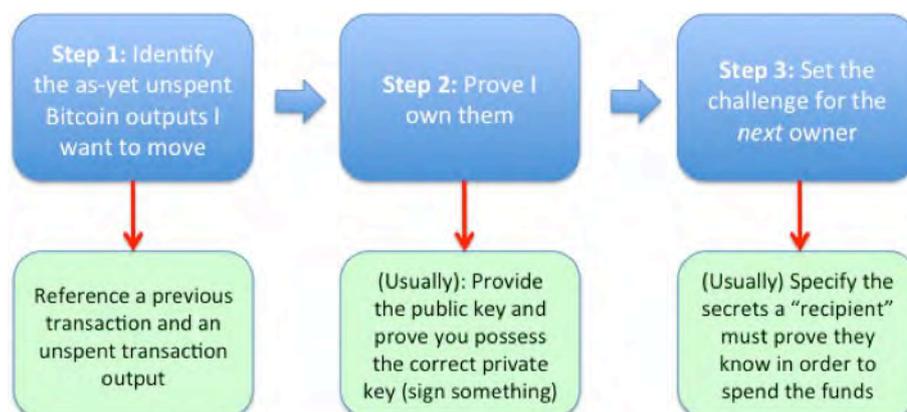


Table courtesy of Bach, A., Corallo, M. Dashjr, L. et al (2014)¹³.

Step Four: Confirmation

11. With Bitcoin, announcing a payment to the recipient's address is almost instantaneous. However, the transaction must still be bundled into a block by miners to begin the confirmation process. On average, it takes approximately 10 minutes for the miners on the Bitcoin network to build (or solve) a given block. Once a transaction in a block has been added to the blockchain, it remains part of the blockchain. All subsequent blocks in the blockchain are built on top of the block containing that particular transaction. Each block added to the blockchain after a block containing a given transaction is considered a **confirmation**¹⁴ of that transaction. A **confirmation** reflects consensus on the network that the particular bitcoins the recipient has received have not been sent to anyone else and are considered the recipient's property. A transaction must be confirmed before the recipient can spend/send the bitcoins he/she has received. The subsequent blocks in the blockchain built on top of the block containing a particular transaction consolidate the confirmation consensus and prevent reversal of the transaction. Users are free to determine how many subsequent blocks, in addition to the initial confirmation, should be added to the blockchain before the transaction is sufficiently confirmed that it is safe to spend/transmit the VC units. Generally, a transaction is not considered to be adequately confirmed until a certain number of confirmations (subsequent blocks)—typically, six—appears on the blockchain.¹⁵

PARTICIPATION WITH INTERMEDIARIES: EMERGING BITCOIN INFRASTRUCTURE

12. A growing number of start-ups have been emerging to provide new VC payments products and services (VCPSS) that facilitate use of decentralised VC payments networks, particularly Bitcoin. Instead of downloading the Bitcoin client or an unhosted wallet and storing and protecting their private keys and conducting transactions themselves, as described above, users (consumers and merchants) can now rely on a variety of third-party businesses that make it much easier to store the VC and conduct decentralised VC transactions. A variety of business models exist with respect to these third parties products and services. Some businesses provide a single type of service, while others offer several types of products and services to their customers. While the decentralised virtual currency “ecosystem” is rapidly evolving, some of these third party VCPSS are described below.

13. **Wallet provider.** Instead of downloading software that creates their addresses themselves, users can now obtain Bitcoin addresses by opening an account at a Bitcoin exchange or online wallet service. And instead of obtaining bitcoins from exchangers and storing them in an unhosted wallet on their own digital devices, they can obtain store the VC in a **hosted wallet**,¹⁶ provided and safeguarded by a **wallet provider**.¹⁷ The wallet provider maintains the customer’s virtual currency balance and generally also provides storage and transaction security. Beyond providing Bitcoin addresses, the wallet provider may offer encryption; multiple key (multi-key) signature protection; backup/cold storage; and mixers. All Bitcoin wallets can interoperate with each other. A wallet provider may provide hot or cold bitcoin storage, with the customer’s retaining his/her private keys and control over transferring the VC. Alternatively, the wallet provider may hold both the public and private keys for the customer’s VC and transfer the VC to third parties at the direction of the customer, to make payments and send remittances. **Many VC exchangers offer wallet services** (i.e., also function as wallet providers), allowing the user to obtain addresses and store his/her VC in an account at the exchange. At present, two models of third-party wallets predominate. In the earlier, more “traditional” wallet hosting services, the customer has his/her own wallet but the file is held on the third-party wallet service’s servers. (There are numerous variations of this model, particularly with regard to whether the host has full control of the private key(s).) In the second model, which most exchanges are currently moving toward, the customer funds are held in pooled accounts, and the company conducts transfers/withdrawals at the customer’s direction. This business model allows more of the VC funds to be held in cold storage, without impairing customer access to his/her VC.

14. A **virtual currency payment processor (a.k.a. third-party payments sender; merchant payments processor)** is an entity that facilitates merchant acceptance—i.e., it is an entity that facilitates the transfer of virtual currency payments from a user (customer) to a merchant or other business or professional that provides consumer goods or services. Typically, payment processors provide software applications or embeddable code that allow the merchant or other business to accept the virtual currency payment on its Internet website or at its brick-and-mortar location, and that either electronically transmit the virtual currency to the merchant’s wallet (hosted by the processor or another wallet provider, or unhosted and held directly by the merchant), or convert some or all of the virtual currency into fiat currency and transmit an e-money payment to the merchant’s account, as directed. Since Bitcoin and other decentralised convertible virtual currencies

are Internet-based payment systems specifically designed to cut out middlemen, it may seem odd to have virtual currency processors as participants in the virtual currency ecosystem. However, processors seek to make it easier for everyday, non-tech-savvy businesses to accept virtual currency payments. Some virtual currency payments processors may offer exchange (conversion) services for merchants that accept convertible virtual currency as payment but fear potential negative volatility of the currency, allowing them for hedging purposes to immediately convert incoming virtual currency into a fiat currency of their choice. Processors also make it easier for (non-tech-savvy) consumers to use virtual currency to purchase goods and services, affording them greater choice in their retail payments methods.

15. **Bitcoin ATM (a.k.a. BTM)** refers to an automated machine used to exchange fiat currency for bitcoin and/or other virtual currency, and vice versa. Depending on its programmed functionality, persons can use a bitcoin ATM to purchase bitcoins (and possibly other virtual currency) (mono-directional machines) or to both purchase virtual currency and cash-out virtual currency for fiat currency by withdrawing the fiat currency in exchange for the convertible virtual currency at the ATM (bi-directional machines –i.e., cash-in/Bitcoin-out or vice versa). The Bitcoin ATM industry is currently dominated by a few large players, but as the sector grows, others may be expected to enter. The number of active (live) Bitcoin ATMs is unclear, but one site reports that as of end-November 2014, there were approximately 300 bitcoin ATMs in operation worldwide. Bitcoin ATM operators charge a fee per transaction, with some Bitcoin ATM manufacturers' taking a commission on the operator's transaction fees.

NOTES

- ¹ Peer-to-peer (P2P) payments are digital payments that a user sends directly to the recipient via the Internet.
- ² At present, all cryptocurrencies are decentralised VCs and all decentralised VCs are cryptocurrencies. However, some centralised cryptocurrencies (i.e., a centralised VC system, or even a fiat-based system) are emerging that use a blockchain-like transaction ledger to handle customer transactions. It is possible that in the relatively near future, not all cryptocurrencies will be decentralised.
- ³ Bitcoin uses a proof-of-work method to verify transactions and create new bitcoins. Some altcoins use proof-of-stake or zero-knowledge proofs for this purpose.
- ⁴ All decentralised VC is convertible, by definition (i.e., there is no central authority that establishes the requirements for redemption).
- ⁵ There are currently two basic models of decentralised virtual currency payments mechanisms: single-currency (a.k.a. currency-specific) VC networks, like Bitcoin, and currency-agnostic VC networks, like Ripple and Ethereum. As the name implies, a **single-currency payments network** handles a given type of decentralised virtual currency. **Currency-agnostic payment platforms**, provide a platform for transacting in any virtual currency or any other tradable value, such as commodities, stock, real estate, etc. For an explanation of how a currency-agnostic VC platform operates, see *The Ripple Protocol: A Deep Dive for Finance Professionals*, available at <https://ripple.com/ripple-deep-dive/>. This citation is provided for information purposes only, and does not represent FATF endorsement of Ripple or any other VCNPPS.

-
- 6 Another trust function typically performed by financial institutions as intermediaries is the guarantee of payment from payor to payee. For traditional electronic payments, financial institutions intermediate transactions by guaranteeing payment (i.e., assuming the buyer's credit risk) and providing for post-transaction dispute resolution. Bitcoin seeks to solve the payment guarantee problem without financial institutions by achieving near real-time settlement and making its transactions irreversible (i.e., not subject to dispute resolution).
- 7 The **blockchain** is the shared Bitcoin transaction register, in the form of a publicly available, shared database with a sequential record of all transactions.
- 8 All Bitcoin transactions are stored publicly and permanently on the blockchain. Anyone accessing the network can see and monitor the balance and transactions of any Bitcoin address, identified by public key, on the blockchain.
- 9 **Miners**, acting as nodes in the network, race to "discover" the next block by solving an increasingly difficult cryptographic puzzle, using a hashing algorithm. Bitcoin mining is a purely mathematical process, analogous to the search for prime using advanced high-performance computers. Bitcoins miners search to find a sequence of data (a 'block') that produces a particular pattern when the Bitcoin 'hash' algorithm is applied to the data. The winner announces the new block to the other nodes and receives new bitcoins as payment. The other nodes verify that the solution complies with all the rules of the Bitcoin protocol and then accept it as the next official entry in the blockchain, starting the process anew.
- 10 **Mining** is the distributed transaction validation process that generates the blockchain and creates new bitcoins.
- 11 A miner is awarded a set number (predetermined by the Bitcoin protocol) of newly created bitcoins, and in some instances, also transaction fees for solving each algorithm that serves to verify and enter payments into the blockchain. An algorithm releases new bitcoins into the network at preset intervals--currently, 50 every 10 minutes, with the pace halving in approximately four-year increments until about 2140. In 2015, 25 bitcoins are awarded to the winning miner. When the total of 21 million bitcoins is in existence, transaction processing will only be rewarded by the transaction fees. The predetermined rate of release of the digital currency is intended to ensure regular growth of the Bitcoin money supply at a predictable rate without interference by third parties, like a central bank, to prevent hyperinflation.
- 12 As noted above, mining involves running a special piece of software on their computers to solve complex algorithms in a "distributed proof-of-work system." The user is awarded a certain number of newly created bitcoins for solving each algorithm.
- 13 Bach, A., Corallo, M. Dashjr, L. et al (2014, *Enabling Blockchain Innovations with Pegged Sidechains*, (October 2014), <https://gandal.wordpress.com/2014/10/26/a-simple-explanation-of-bitcoin-sidechains/>).
- 14 **Confirmation** refers to the point when the transaction is validated by a miner and recorded in the blockchain.
- 15 While some merchants require VC users to wait until the VC transaction is confirmed a set number of times before treating the payment transaction as settled and processing the customer's order, for low value transactions, where the fraud risk is not great, some merchants treat receipt of the bitcoins, rather than confirmation, as valid payment.
- 16 A **hosted wallet** is a virtual currency wallet held by a third-party wallet provider (which may be an exchange).

¹⁷ **A wallet provider** is an entity that provides a virtual currency wallet for holding, storing and transferring bitcoins or other virtual currency.

Regulation of virtual assets

 Send  Print  Tweet

Paris, France, 19 October 2018 - Virtual assets and related financial services have the potential to spur financial innovation and efficiency and improve financial inclusion, but they also create new opportunities for criminals and terrorists to launder their proceeds or finance their illicit activities. The FATF has therefore been actively monitoring risks in this area, and issued guidance on a risk-based approach to virtual currencies in 2015. There is an urgent need for all countries to take coordinated action to prevent the use of virtual assets for crime and terrorism.

The FATF Recommendations set out comprehensive requirements for combating money laundering and terrorist financing that apply to all forms of financial activity—including those that make use of virtual assets. However, governments and the private sector have asked for greater clarity about exactly which activities the FATF standards apply to in this context. The Risk-based Approach requires jurisdictions to identify money laundering and terrorist financing risks and take appropriate action to mitigate those risks. This includes identifying and mitigating illicit financing risks associated with new products or business practices, and other activities not explicitly referred to in the FATF Recommendations.

Given the urgent need for an effective global, risk-based response to the AML/CFT risks associated with virtual asset financial activities, the FATF has adopted changes to the FATF Recommendations and Glossary that clarify how the Recommendations apply in the case of financial activities involving virtual assets. These changes add to the Glossary new definitions of “virtual assets” and “virtual asset service providers” – such as exchanges, certain types of wallet providers, and providers of financial services for Initial Coin Offerings (ICOs). These changes make clear that jurisdictions should ensure that virtual asset service providers are subject to AML/CFT regulations, for example conducting customer due diligence including ongoing monitoring, record-keeping, and reporting of suspicious transactions. They should be licensed or registered and subject to monitoring to ensure compliance. The FATF will further elaborate on how these requirements should be applied in relation to virtual assets.

All jurisdictions should urgently take legal and practical steps to prevent the misuse of virtual assets. This includes assessing and understanding the risks associated with virtual assets in their jurisdictions, applying risk-based AML/CFT regulations to virtual asset service providers and identifying effective systems to conduct risk-based monitoring or supervision of virtual asset service providers. Some jurisdictions already regulate virtual asset activity in accordance with the 2015 guidance. Today’s clarifications to the FATF Standards are largely compatible with their existing regulatory requirements. The FATF emphasises that jurisdictions have flexibility to decide under which AML/CFT category of regulated activities virtual asset service providers should be regulated, e.g. as financial institutions, DNFBPs, or as another, distinctive category.

The FATF uses the term “virtual asset” to refer to digital representations of value that can be digitally traded or transferred and can be used for payment or investment purposes, including digital representations of value that function as a medium of exchange, a unit of account, and/or a store of value. The FATF emphasises that virtual assets are distinct from fiat currency (a.k.a. “real currency,” “real money,” or “national currency”), which is the money of a country that is designated as its legal tender.

The FATF Recommendations require monitoring or supervision only for the purposes of AML/CFT, and do not imply that virtual asset service providers are (or should be) subject to stability or consumer/investor protection safeguards, nor do they imply any consumer or investor protection safeguards. At this time, virtual asset service providers in most jurisdictions are not regulated for the purposes of financial stability or for investor and consumer protection.

The FATF Standards permit jurisdictions to prohibit certain activities based on risk and scope in that jurisdiction (e.g. casinos, in jurisdictions where gambling is illegal) and, provided the prohibition is enforced, does not require jurisdictions to have measures to regulate those prohibited activities. Some countries may decide to prohibit virtual assets based on their own assessment of risk.

The FATF will provide clarification to jurisdictions in managing the ML and TF risks of virtual assets, while creating a sound AML/CFT regulatory environment in which companies are free to innovate. As part of a staged approach, the FATF will prepare updated guidance on a risk-based approach to regulating virtual asset service providers, including their supervision and monitoring; and guidance for operational and law enforcement authorities on identifying and investigating illicit activity involving virtual assets.

In light of the rapid development of the range of financial functions served by virtual assets, the FATF will also review the scope of activities and operations covered in the amended Recommendations and Glossary in the next 12 months and consider whether further updates are necessary to ensure the FATF Standards stay relevant.

More on:

- [FATF Recommendations](#)
- [Outcomes FATF Plenary, 19 October 2018](#)

[← FATF Recommendations](#)

INTERPRETIVE NOTE TO RECOMMENDATION 15

1. For the purposes of applying the FATF Recommendations, countries should consider virtual assets as “property,” “proceeds,” “funds,” “funds or other assets,” or other “corresponding value.” Countries should apply the relevant measures under the FATF Recommendations to virtual assets and virtual asset service providers (VASPs)
2. In accordance with Recommendation 1, countries should identify, assess, and understand the money laundering and terrorist financing risks emerging from virtual asset activities and the activities or operations of VASPs. Based on that assessment, countries should apply a risk-based approach to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. Countries should require VASPs to identify, assess, and take effective action to mitigate their money laundering and terrorist financing risks.
3. VASPs should be required to be licensed or registered. At a minimum, VASPs should be required to be licensed or registered in the jurisdiction(s) where they are created⁴⁰. In cases where the VASP is a natural person, they should be required to be licensed or registered in the jurisdiction where their place of business is located. Jurisdictions may also require VASPs that offer products and/or services to customers in, or conduct operations from, their jurisdiction to be licensed or registered in this jurisdiction. Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a VASP. Countries should take action to identify natural or legal persons that carry out VASP activities without the requisite license or registration, and apply appropriate sanctions.
4. A country need not impose a separate licensing or registration system with respect to natural or legal persons already licensed or registered as financial institutions (as defined by the FATF Recommendations) within that country, which, under such license or registration, are permitted to perform VASP activities and which are already subject to the full range of applicable obligations under the FATF Recommendations.
5. Countries should ensure that VASPs are subject to adequate regulation and supervision or monitoring for AML/CFT and are effectively implementing the relevant FATF Recommendations, to mitigate money laundering and terrorist financing risks emerging from virtual assets. VASPs should be subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements. VASPs should be supervised or monitored by a competent authority (not a SRB), which should conduct risk-based supervision or monitoring. Supervisors should have adequate powers to supervise or monitor and ensure compliance by VASPs with requirements to combat money laundering and terrorist financing including the authority to conduct inspections, compel the production of information, and impose sanctions. Supervisors should have powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the VASP’s license or registration, where applicable.
6. Countries should ensure that there is a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with VASPs that fail to

⁴⁰ References to creating a legal person include incorporation of companies or any other mechanism that is used.

comply with AML/CFT requirements, in line with Recommendation 35. Sanctions should be applicable not only to VASPs, but also to their directors and senior management.

7. With respect to the preventive measures, the requirements set out in Recommendations 10 to 21 apply to VASPs, subject to the following qualifications:
 - (a) R. 10 – The occasional transactions designated threshold above which VASPs are required to conduct CDD is USD/EUR 1 000.
 - (b) R. 16 – Countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information⁴¹ on virtual asset transfers, submit⁴² the above information to the beneficiary VASP or financial institution (if any) immediately and securely, and make it available on request to appropriate authorities. Countries should ensure that beneficiary VASPs obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers and make it available on request to appropriate authorities. Other requirements of R. 16 (including monitoring of the availability of information, and taking freezing action and prohibiting transactions with designated persons and entities) apply on the same basis as set out in R. 16. The same obligations apply to financial institutions when sending or receiving virtual asset transfers on behalf of a customer.
8. Countries should rapidly, constructively, and effectively provide the widest possible range of international cooperation in relation to money laundering, predicate offences, and terrorist financing relating to virtual assets, on the basis set out in Recommendations 37 to 40. In particular, supervisors of VASPs should exchange information promptly and constructively with their foreign counterparts, regardless of the supervisors' nature or status and differences in the nomenclature or status of VASPs.

⁴¹ As defined in INR. 16, paragraph 6, or the equivalent information in a virtual asset context.

⁴² The information can be submitted either directly or indirectly. It is not necessary for this information to be attached directly to the virtual asset transfers.

FATF



GUIDANCE FOR A RISK-BASED APPROACH

VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS



JUNE 2019

Appendix E



The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit www.fatf-gafi.org

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2019), *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, FATF, Paris,
www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html

© 2019 FATF/OECD. All rights reserved.

No reproduction or translation of this publication may be made without prior written permission.

Applications for such permission, for all or part of this publication, should be made to the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France (fax: +33 1 44 30 61 37 or e-mail: contact@fatf-gafi.org)

Photocredits coverphoto ©Getty Images

Table of contents

Acronyms	3
Executive summary	4
Section I - Introduction	6
Background	6
Purpose of the Guidance.....	7
Scope of the Guidance.....	7
Structure	9
Section II – Scope of FATF Standards	11
Initial Risk Assessment	11
FATF Definitions and Features of the VASP Sector Relevant for AML/CFT	13
Section III – Application of FATF Standards to Countries and Competent Authorities	19
Application of the Recommendations in the Context of VAs and VASPs	19
Risk-Based Approach and National Co-ordination	19
Treatment of Virtual Assets: Interpreting the Funds- or Value-Based Terms.....	20
Licensing or Registration.....	22
Supervision or Monitoring.....	23
Preventive Measures.....	24
Transparency and Beneficial Ownership of Legal Persons and Arrangements.....	32
Operational and Law Enforcement	32
International Co-operation.....	33
DNFBPs that Engage in or Provide Covered VA Activities	34
Risk-Based Approach to Supervision or Monitoring of VASPs	34
Understanding the ML/TF Risks	34
Mitigating the ML/TF Risks	36
General Approach.....	37
Guidance	38
Training	38
Information Exchange	39
Section IV – Application of FATF Standards to VASPs and other obliged entities that Engage in or Provide Covered VA Activities	40
Section V – Country Examples of Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers	46
Summary of Jurisdictional Approaches to Regulating and Supervising VA Activities and VASPs ..	46
Italy	46
Norway	47

Sweden.....	48
Finland.....	48
Mexico.....	49
Japan.....	49
United States.....	50
Annex A. Recommendation 15 and its Interpretive Note and FATF Definitions	55
Recommendation 15 – New Technologies.....	55
Interpretative Note to Recommendation 15	55
FATF Glossary.....	57

ACRONYMS

AEC	Anonymity-Enhanced Cryptocurrency
AML	Anti-Money Laundering
CDD	Customer Due Diligence
CFT	Countering the Financing of Terrorism
DNFBP	Designated Non-Financial Business and Profession
ICO	Initial Coin Offering
ML	Money Laundering
MSB	Money Services Business
MVTS	Money or Value Transfer Service
OTC	Over-the-Counter
P2P	Peer-to-Peer
RBA	Risk-Based Approach
TF	Terrorist Financing
VA	Virtual Asset
VASP	Virtual Asset Service Provider

EXECUTIVE SUMMARY

In October 2018, the FATF adopted changes to its Recommendations to explicitly clarify that they apply to financial activities involving virtual assets, and also added two new definitions in the Glossary, “virtual asset” (VA) and “virtual asset service provider” (VASP). The amended FATF Recommendation 15 requires that VASPs be regulated for anti-money laundering and combating the financing of terrorism (AML/CFT) purposes, licenced or registered, and subject to effective systems for monitoring or supervision.

In June 2019, the FATF adopted an Interpretive Note to Recommendation 15 to further clarify how the FATF requirements should apply in relation to VAs and VASPs, in particular with regard to the application of the risk-based approach (RBA) to VA activities or operations and VASPs; supervision or monitoring of VASPs for AML/CFT purposes; licensing or registration; preventive measures, such as customer due diligence, recordkeeping, and suspicious transaction reporting, among others; sanctions and other enforcement measures; and international co-operation.

The FATF also adopted the present Guidance¹ on the application of the RBA to VAs and VASPs In June 2019. It is intended to help both national authorities in understanding and developing regulatory and supervisory responses to VA activities and VASPs, and to help private sector entities seeking to engage in VA activities, in understanding their AML/CFT obligations and how they can effectively comply with these requirements.

This Guidance outlines the need for countries and VASPs, and other entities involved in VA activities, to understand the ML/TF risks associated with their activities and take appropriate mitigating measures to address them. In particular, the Guidance provides examples of risk indicators that should specifically be considered in a VA context, with an emphasis on factors that would further obfuscate transactions or inhibit VASPs’ ability to identify customers.

The Guidance examines how VA activities and VASPs fall within the scope of the FATF Recommendations. It discusses the five types of activities covered by the VASP definition and provides examples of VA-related activities that would fall within the VASP definition and that would be excluded from the FATF scope. In that respect, it highlights the key elements required to qualify as a VASP, namely acting as a business on behalf of the customers and actively facilitating VA-related activities.

The Guidance describes the application of the FATF Recommendations to countries and competent authorities; as well as to VASPs and other obliged entities that engage into VA activities, including financial institutions such as banks and securities broker-dealers, among others. Almost all of the FATF Recommendations are directly relevant to address the ML/TF risks associated with VAs and VASPs, while other Recommendations are less directly or explicitly linked to VAs or VASPs, though are still relevant and applicable. VASPs therefore have the same full set of obligations as financial institutions or DNFBPs.

¹ This Guidance updates the 2015 [FATF Guidance for a Risk-Based Approach to Virtual Currencies](#).

The Guidance details the full range of obligations applicable to VASPs as well as to VAs under the FATF Recommendations, following a Recommendation-by-Recommendation approach. This includes clarifying that all of the funds or value-based terms in the FATF Recommendations (*e.g.*, “property,” “proceeds,” “funds,” “funds or other assets,” and other “corresponding value”) include VAs. Consequently, countries should apply all of the relevant measures under the FATF Recommendations to VAs, VA activities, and VASPs.

The Guidance explains the VASP registration or licensing requirements, in particular how to determine in which country/ies VASPs should be registered or licensed – at a minimum where they were created; or in the jurisdiction where their business is located in cases where they are a natural person, but jurisdictions can also chose to require VASPs to be licensed or registered before conducting business in their jurisdiction or from their jurisdiction. The Guidance further underlines that national authorities are required to take action to identify natural or legal persons that carry out VA activities without the requisite license or registration. This would be equally applicable by countries which have chosen to prohibit VA and VA activities at national level.

Regarding VASP supervision, the Guidance makes clear that only competent authorities can act as VASP supervisory or monitoring bodies, and not self-regulatory bodies. They should conduct risk-based supervision or monitoring, with adequate powers, including the power to conduct inspections, compel the production of information and impose sanctions. There is a specific focus on the importance of international co-operation between supervisors, given the cross-border nature of VASPs’ activities and provision of services.

The Guidance makes clear that VASPs, and other entities involved in VA activities, need to apply all the preventive measures described in FATF Recommendations 10 to 21. The Guidance explains how these obligations should be fulfilled in a VA context and provides clarifications regarding the specific requirements applicable regarding the USD/EUR 1 000 threshold for VA occasional transactions, above which VASPs must conduct customer due diligence (Recommendation 10); and the obligation to obtain, hold, and transmit required originator and beneficiary information, immediately and securely, when conducting VA transfers (Recommendation 16). As the guidance makes clear, relevant authorities should co-ordinate to ensure this can be done in a way that is compatible with national data protection and privacy rules.

Finally, the Guidance provides examples of jurisdictional approaches to regulating, supervising, and enforcing VA activities, VASPs, and other obliged entities for AML/CFT.

SECTION I - INTRODUCTION

Background

1. New technologies, products, and related services have the potential to spur financial innovation and efficiency and improve financial inclusion, but they also create new opportunities for criminals and terrorists to launder their proceeds or finance their illicit activities. The risk-based approach is central to the effective implementation of the revised Financial Action Task Force (FATF) International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, which FATF members adopted in 2012, and the FATF therefore actively monitors the risks relating to new technologies.
2. In June 2014, the FATF issued [Virtual Currencies: Key Definitions and Potential AML/CFT Risks](#) in response to the emergence of virtual currencies and their associated payment mechanisms for providing new methods of transmitting value over the Internet. In June 2015, the FATF issued the [Guidance for a Risk-Based Approach to Virtual Currencies](#) (the 2015 VC Guidance) as part of a staged approach to addressing the money laundering and terrorist financing (ML/TF) risks associated with virtual currency payment products and services.
3. The 2015 VC Guidance focuses on the points where virtual currency activities intersect with and provide gateways to and from (*i.e.*, the on and off ramps to) the traditional regulated financial system, in particular convertible virtual currency exchangers. In recent years, however, the virtual asset space has evolved to include a range of new products and services, business models, and activities and interactions, including virtual-to-virtual asset transactions.
4. In particular, the virtual asset ecosystem has seen the rise of anonymity-enhanced cryptocurrencies (AECs), mixers and tumblers, decentralized platforms and exchanges, and other types of products and services that enable or allow for reduced transparency and increased obfuscation of financial flows, as well as the emergence of other virtual asset business models or activities such as initial coin offerings (ICOs) that present ML/TF risks, including fraud and market manipulation risks. Further, new illicit financing typologies continue to emerge, including the increasing use of virtual-to-virtual layering schemes that attempt to further obfuscate transactions in a comparatively easy, cheap, and secure manner.
5. Given the development of additional products and services and the introduction of new types of providers in this space, the FATF recognized the need for further clarification on the application of the Standards to new technologies and providers. In particular, in October 2018, the FATF adopted two new Glossary definitions—“virtual asset” (VA) and “virtual asset service provider” (VASP)—and updated Recommendation 15 (see Annex A). The objectives of those changes were to further clarify the application of the FATF Standards to VA activities and VASPs in order to ensure a level regulatory playing field for VASPs globally and to assist jurisdictions in mitigating the ML/TF risks associated with VA activities and in protecting the integrity of the global financial system. The FATF also clarified that the Standards apply to both virtual-to-virtual and virtual-to-fiat transactions and interactions involving VAs.
6. In June 2019, the FATF adopted an Interpretive Note to Recommendation 15 (INR. 15) to further clarify how the FATF requirements should apply in relation to VAs and VASPs, in particular with regard to the application of the risk-based approach to VA activities or operations and VASPs; supervision or monitoring of VASPs for anti-money laundering and countering the financing of terrorism (AML/CFT) purposes; licensing or registration; preventive measures, such as customer due diligence, recordkeeping, and suspicious transaction reporting, among others; sanctions and other enforcement measures; and international co-operation (see Annex A).
7. The FATF adopted this Guidance at its June 2019 Plenary.

Purpose of the Guidance

8. This updated Guidance expands on the 2015 VC Guidance and further explains the application of the risk-based approach to AML/CFT measures for VAs; identifies the entities that conduct activities or operations relating to VA—*i.e.*, VASPs; and clarifies the application of the FATF Recommendations to VAs and VASPs. The Guidance is intended to help national authorities in understanding and developing regulatory responses to covered VA activities and VASPs, including by amending national laws, where applicable, in their respective jurisdictions in order to address the ML/TF risks associated with covered VA activities and VASPs.
9. The Guidance also is intended to help private sector entities seeking to engage in VA activities or operations as defined in the FATF Glossary to better understand their AML/CFT obligations and how they can effectively comply with the FATF requirements. It provides guidelines to countries, competent authorities, and industry for the design and implementation of a risk-based AML/CFT regulatory and supervisory framework for VA activities and VASPs, including the application of preventive measures such as customer due diligence, record-keeping, and suspicious transaction reporting, among other measures.
10. The Guidance incorporates the terms adopted by the FATF in October 2018 and readers are referred to the FATF Glossary definitions for “virtual asset” and “virtual asset service provider” (Annex A).
11. The Guidance seeks to explain how the FATF Recommendations should apply to VA activities and VASPs; provides examples, where relevant or potentially most useful; and identifies obstacles to applying mitigating measures alongside potential solutions. It is intended to serve as a complement to Recommendation 15 on New Technologies (R. 15) and its Interpretive Note, which describe the full range of obligations applicable to VASPs as well as to VAs under the FATF Recommendations, including the Recommendations relating to “property,” “proceeds,” “funds,” “funds or other assets,” and other “corresponding value.” In doing so, the Guidance supports the effective implementation of national AML/CFT measures for the regulation and supervision of VASPs (as well as other obliged entities) and the covered VA activities in which they engage and the development of a common understanding of what a risk-based approach to AML/CFT entails.
12. While the FATF notes that some governments are considering a range of regulatory responses to VAs and to the regulation of VASPs, many jurisdictions do not yet have in place effective AML/CFT frameworks for mitigating the ML/TF risks associated with VA activities in particular, even as VA activities develop globally and VASPs increasingly operate across jurisdictions. The rapid development, increasing functionality, growing adoption, and global, cross-border nature of VAs therefore makes the urgent action by countries to mitigate the ML/TF risks presented by VA activities and VASPs a key priority of the FATF. While this Guidance is intended to facilitate the implementation of the risk-based approach to covered VA activities and VASPs for AML/CFT purposes, the FATF recognizes that other types of policy considerations may come into play and shape the regulatory response to the VASP sector in individual jurisdictions.

Scope of the Guidance

13. The FATF Recommendations require all jurisdictions to impose specified, activities-based AML/CFT requirements on financial institutions (FIs) and designated non-financial businesses and professions (DNFBPs) and ensure their compliance with those obligations. The FATF has agreed that all of the funds- or value-based terms in the FATF Recommendations (*e.g.*, “property,” “proceeds,” “funds,” “funds or other assets,” and other “corresponding value”) include VAs and that countries should apply all of the relevant measures under the FATF

- Recommendations to VAs, VA activities, and VASPs. The primary focus of the Guidance is to describe how the Recommendations apply to VAs, VA activities, and VASPs in order to help countries better understand how they should implement the FATF Standards effectively.
14. Further, the Guidance focuses on VAs that are convertible for other funds or value, including both VAs that are convertible to another VA and VAs that are convertible to fiat or that intersect with the fiat financial system, having regard to the VA and VASP definitions. It does not address other regulatory matters that are potentially relevant to VAs and VASPs (*e.g.*, consumer protection, prudential safety and soundness, tax, anti-fraud or anti-market manipulation issues, network IT security standards, or financial stability concerns).
 15. The Guidance recognizes that an effective risk-based approach will reflect the nature, diversity, and maturity of a country's VASP sector, the risk profile of the sector, the risk profile of individual VASPs operating in the sector and the legal and regulatory approach in the country, taking into account the cross-border, Internet-based nature and global reach of most VA activities. The Guidance sets out different elements that countries and VASPs should consider when designing and implementing a risk-based approach. When considering the general principles outlined in the Guidance, national authorities will have to take into consideration their national context, including the supervisory approach and legal framework as well as the risks present in their jurisdiction, again in light of the potentially global reach of VA activities.
 16. The Guidance takes into account that just as illicit actors can abuse any institution that engages in financial activities, illicit actors can abuse VASPs engaging in VA activities, for ML, TF, sanctions evasion, fraud, and other nefarious purposes. The 2015 VC Guidance, the 2018 FATF Risk, Trends, and Methods Group papers relating to this topic, and FATF reports and statements relating to the ML/TF risks associated with VAs, VA activities, and/or VASPs,² for example, highlight and provide further context regarding the ML/TF risks associated with VA activities. While VAs may provide another form of value for conducting ML and TF, and VA activities may serve as another mechanism for the illegal transfer of value or funds, countries should not necessarily categorize VASPs or VA activities as inherently high ML/TF risks. The cross-border nature of, potential enhanced-anonymity associated with, and non-face-to-face business relationships and transactions facilitated by VA activities should nevertheless inform a country's assessment of risk. The extent and quality of a country's regulatory and supervisory framework as well as the implementation of risk-based controls and mitigating measures by VASPs also influence the overall risks and threats associated with covered VA activities. The Guidance also recognizes that despite these measures, there may still be some residual risk, which competent authorities and VASPs should consider in devising appropriate solutions.
 17. The Guidance recognizes that "new" or innovative technologies or mechanisms for engaging in or that facilitate financial activity may not automatically constitute "better" approaches and that jurisdictions should also assess the risks arising from and appropriately mitigate the risks such new methods of performing a traditional or already-regulated financial activity, such as the use of VAs in the context of payment services or securities activities, as well.
 18. Other stakeholders, including FIs and other obliged entities that provide banking services to VASPs or to customers involved in VA activities or that engage in VASP activities themselves should also consider the aforementioned factors. FIs should apply a risk-based approach when considering establishing or continuing relationships with VASPs or customers involved in VA activities, evaluate the ML/TF risks of the business relationship, and assess whether those risks can be appropriately mitigated and managed (see Section IV). It is important that FIs

² See, for example, the [July 2018 FATF report to G-20 Finance Ministers and Central Bank Governors](#); the [February 2019 FATF public statement on mitigating risks from virtual assets](#); and the [April 2019 FATF report to G-20 Finance Ministers and Central Bank Governors](#).

- apply the risk-based approach properly and do not resort to the wholesale termination or exclusion of customer relationships within the VASP sector without a proper risk assessment.
19. In considering the Guidance, countries, VASPs and other obliged entities that engage in or provide covered VA activities should recall the key principles underlying the design and application of the FATF Recommendations and that are relevant in the VA context:
- a) *Functional equivalence and objectives-based approach.* The FATF requirements, including as they apply in the VA space, are compatible with a variety of different legal and administrative systems. They broadly explain what must be done but not in an overly-specific manner about how implementation should occur in order to allow for different options, where appropriate. Any clarifications to the requirements should not require jurisdictions that have already adopted adequate measures to achieve the objectives of the FATF Recommendations to change the form of their laws and regulations. The Guidance seeks to support ends-based or objectives-based implementation of the relevant FATF Recommendations rather than impose a rigid prescriptive one-size-fits-all regulatory regime across all jurisdictions.
 - b) *Technology-neutrality and future-proofing.* The requirements applicable to VAs, as value or funds, to covered VA activities, and to VASPs apply irrespective of the technological platform involved. Equally, the requirements are not intended to give preference to specific products, services, or solutions offered by commercial providers, including technological implementation solutions that aim to assist providers in complying with their AML/CFT obligations. Rather, the requirements are intended to have sufficient flexibility that countries and relevant entities can apply them to existing technologies as well as to evolving and emerging technologies without requiring additional revisions.
 - c) *Level-playing field.* Countries and their competent authorities should treat all VASPs on an equal footing from a regulatory and supervisory perspective in order to avoid jurisdictional arbitrage. As with FIs and DNFBPs, countries should therefore subject VASPs to AML/CFT requirements that are functionally equivalent to other entities when they offer similar products and services and based on the activities in which the entities engage.
20. This Guidance is non-binding and does not overrule the purview of national authorities, including on their assessment and categorization of VASPs, VAs, and VA activities, as per the country or regional circumstances, the prevailing ML/TF risks, and other contextual factors. It draws on the experiences of countries and of the private sector and is intended to assist competent authorities, VASPs, and relevant FIs (*e.g.*, banks engaging in covered VA activities) in effectively implementing the FATF Recommendations using a risk-based approach.

Structure

21. This Guidance is organized as follows: Section II examines how VA activities and VASPs fall within the scope of the FATF Recommendations; Section III describes the application of the FATF Recommendations to countries and competent authorities; Section IV explains the application of the FATF Recommendations to VASPs and other obliged entities that engage in or provide VA covered activities, including FIs such as banks and securities broker-dealers, among others; and Section V provides examples of jurisdictional approaches to regulating, supervising, and enforcing covered VA activities and VASPs (and other obliged entities) for AML/CFT.
22. Annexes A, B, and C include relevant resources that augment this Guidance, including the June 2014 *FATF Virtual Currencies: Key Definitions and Potential AML/CFT Risks* paper, the June

2015 VC Guidance, the updated text of Recommendation 15 and its Interpretive Note, and the “virtual asset” and “virtual asset service provider” definitions within the FATF Glossary.

SECTION II – SCOPE OF FATF STANDARDS

23. Section II discusses the applicability of the risk-based approach to VA activities and VASPs and explains how these activities and providers should be subject to AML/CFT requirements under the international standards. As described in paragraph 2 of INR. 15, VASPs are subject to the relevant measures under the FATF Recommendations based on the types of activities in which they engage. Similarly, VAs are captured by the relevant measures under the FATF Recommendations that relate to funds or value, broadly, or that specifically reference funds- or value-based terms.
24. It should be underscored that when VASPs engage in traditional fiat-only activities or fiat-to-fiat transactions (which are outside the scope of the virtual-to-virtual and virtual-to-fiat activities covered by the VASP definition), they are of course subject to the same measures as any other equivalent traditional institution or entity normally would be under the FATF standards.

Initial Risk Assessment

25. The FATF Recommendations do not predetermine any sector as higher risk. The standards identify sectors that may be vulnerable to ML and TF; however the overall risk should be determined through an assessment of the sector—in this case, the VASP sector—at a national level. Different entities within a sector may pose a higher or lower risk depending on a variety of factors, including products, services, customers, geography, and the strength of the entity's compliance program. Recommendation 1 sets out the scope of the application of the risk-based approach as follows: who should be subject to a country's regime; how those subject to the AML/CFT regime should be supervised or monitored for compliance with the regime; how those subject to the AML/CFT regime should be required to comply; and consideration of the engagement in customer relationships by VASPs and other obliged entities involved in covered VA activities. Further, the FATF does not support the wholesale termination or restriction of business relationships with a particular sector (*e.g.*, FI relationships with VASPs, where relevant) to avoid, rather than manage, risk in line with the FATF's risk-based approach.
26. The FATF has assessed that ML/TF risks exist in relation to VAs, VA financial activities or operations, and VASPs. Accordingly, under the risk-based approach and in accordance with paragraph 2 of INR. 15, countries should identify, assess, and understand the ML/TF risks emerging from this space and focus their AML/CFT efforts on potentially higher-risk VAs, covered VA activities, and VASPs. Similarly, countries should require VASPs (as well as other obliged entities that engage in VA financial activities or operations or provide VA products or services) to identify, assess, and take effective action to mitigate their ML/TF risks.
27. A VASP's risk assessment should take into account all of the risk factors that the VASP as well as its competent authorities consider relevant, including the types of services, products, or transactions involved; customer risk; geographical factors; and type(s) of VA exchanged, among other factors.
28. As with many financial payments methods, for example, VAs can enable non-face-to-face business relationships. Further, VAs can be used to quickly move funds globally and to facilitate a range of financial activities—from money or value transfer services to securities, commodities or derivatives-related activity, among others. Thus, the absence of face-to-face contact in VA financial activities or operations may indicate higher ML/TF risks. Similarly, VA products or services that facilitate pseudonymous or anonymity-enhanced transactions also pose higher ML/TF risks, particularly if they inhibit a VASP's ability to identify the beneficiary. The latter is especially concerning in the context of VAs, which are cross-border in nature. If customer identification and verification measures do not adequately address the risks

associated with non-face-to-face or opaque transactions, the ML/TF risks increase, as does the difficulty in tracing the associated funds and identifying transaction counterparties.

29. The extent to which users can use VAs or VASPs globally for making payments or transferring funds is also an important factor that countries should take into account when determining the level of risk. Illicit users of VAs, for example, may take advantage of the global reach and transaction speed that VAs provide as well as of the inadequate regulation or supervision of VA financial activities and providers across jurisdictions, which creates an inconsistent legal and regulatory playing field in the VA ecosystem. As with other mobile or Internet-based payment services and mechanisms that can be used to transfer funds globally or in a wide geographical area with a large number of counterparties, VAs can be more attractive to criminals for ML/TF purposes than purely domestic business models.
30. In addition, VASPs located in one jurisdiction may offer their products and services to customers located in another jurisdiction where they may be subject to different AML/CFT obligations and oversight. This is of concern where the VASP is located in a jurisdiction with weak or even non-existent AML/CFT controls. Similarly, the sheer range of providers in the VA space and their presence across several, if not nearly all, jurisdictions can increase the ML/TF risks associated with VAs and VA financial activities due to potential gaps in customer and transaction information. This is a particular concern in the context of cross-border transactions and when there is a lack of clarity on which entities or persons (natural or legal) involved in the transaction are subject to AML/CFT measures and which countries are responsible for regulating (including licensing and/or registering) and supervising or monitoring those entities for compliance with their AML/CFT obligations.
31. In addition to consulting the previous FATF works on this subject,³ countries and VASPs should consider the following elements, for example, when identifying, assessing, and determining how best to mitigate the risks associated with covered VA activities and the provision of VASP products or services:
 - a) The potentially higher risks associated both with VAs that move value into and out of fiat currency and the traditional financial system and with virtual-to-virtual transactions;
 - b) The risks associated with centralised and decentralised VASP business models;
 - c) The specific types of VAs that the VASP offers or plans to offer and any unique features of each VA, such as AECs, embedded mixers or tumblers, or other products and services that may present higher risks by potentially obfuscating the transactions or undermining a VASP's ability to know its customers and implement effective customer due diligence (CDD) and other AML/CFT measures;
 - d) The specific business model of the VASP and whether that business model introduces or exacerbates specific risks;
 - e) Whether the VASP operates entirely online (*e.g.*, platform-based exchanges) or in person (*e.g.*, trading platforms that facilitate peer-to-peer exchanges or kiosk-based exchanges);
 - f) Exposure to Internet Protocol (IP) anonymizers such as The Onion Router (TOR) or Invisible Internet Project (I2P), which may further obfuscate

³ For example, the 2015 VC Guidance, 2018 FATF Risk, Trends, and Methods Group papers relating to this topic, and FATF statements and reports relating to the ML/TF risks associated with VAs, VA activities, and/or VASPs.

transactions or activities and inhibit a VASP's ability to know its customers and implement effective AML/CFT measures;

- g) The potential ML/TF risks associated with a VASP's connections and links to several jurisdictions;
 - h) The nature and scope of the VA account, product, or service (*e.g.*, small value savings and storage accounts that primarily enable financially-excluded customers to store limited value);
 - i) The nature and scope of the VA payment channel or system (*e.g.*, open- versus closed-loop systems or systems intended to facilitate micro-payments or government-to-person/person-to-government payments); as well as
 - j) Any parameters or measures in place that may potentially lower the provider's (whether a VASP or other obliged entity that engages in VA activities or provides VA products and services) exposure to risk (*e.g.*, limitations on transactions or account balance).
32. Some countries may decide to prohibit VA activities or VASPs, based on their assessment of risk and national regulatory context or in order to support other policy goals not addressed in this Guidance (*e.g.*, consumer protection, safety and soundness, or monetary policy). In such cases, some of the specific requirements of R. 15 would not apply, but jurisdictions would still need to assess the risks associated with covered VA activities or providers and have tools and authorities in place to take action for non-compliance with the prohibition (see sub-section 3.1.1.).

FATF Definitions and Features of the VASP Sector Relevant for AML/CFT

33. The FATF Recommendations require all jurisdictions to impose specified AML/CFT requirements on FIs and DNFBPs and ensure their compliance with those obligations. In the Glossary, the FATF defines:
- a) "Financial institution" as any natural or legal person who conducts as a business one or more of several specified activities or operations for or on behalf of a customer;
 - b) "Virtual asset" as a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations; and
 - c) "Virtual asset service provider" as any natural or legal person who is not covered elsewhere under the Recommendations and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:
 - i. Exchange between virtual assets and fiat currencies;
 - ii. Exchange between one or more forms of virtual assets;

- iii. Transfer⁴ of virtual assets; and
 - iv. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets;
 - v. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.
34. Notably, the scope of the FATF definition includes both virtual-to-virtual and virtual-to-fiat transactions or financial activities or operations.
35. Depending on their particular financial activities, VASPs include VA exchanges and transfer services; some VA wallet providers, such as those that host wallets or maintain custody or control over another natural or legal person's VAs, wallet(s), and/or private key(s); providers of financial services relating to the issuance, offer, or sale of a VA (such as in an ICO); and other possible business models.
36. When determining whether a specific activity or entity falls within the scope of the definition and is therefore subject to regulation, countries should consider the wide range of various VA services or business models that exist in the VA ecosystem and, in particular, consider their functionality or the financial activities that they facilitate in the context of the covered VA activities (*i.e.*, items (i) through (v) described in the VASP definition above). Further, countries should consider whether the activities involve a natural or legal person that conducts as a business the five functional activities described for or on behalf of another natural or legal person, both of which are essential elements to the definition and the latter of which implies a certain level of "custody" or "control" of the virtual asset, or "ability to actively facilitate the financial activity" on the part of the natural or legal person that conducts the business for a customer.
37. For example, exchange between virtual assets and fiat currencies (item (i)), exchange between one or more forms of virtual assets (item (ii)), and transfer of virtual assets (item (iii)), including from one hosted wallet to another wallet owned by the same person, potentially apply to various VA exchange and transfer activities. Exchanges or exchangers can exist in various forms and business models and generally provide third-party services that enable their customers to buy and sell VAs in exchange for traditional fiat currency, another VA, or other assets or commodities.⁵ Exchange and/or transfer business models can include "traditional" VA exchanges or VA transfer services that actively facilitate the exchange of VA for real currency or other forms of VA and/or for precious metals for remuneration (*e.g.* for a fee, commission, spread, or other benefit). These models typically accept a wide range of payment methods, including cash, wires, credit cards, and VAs. Traditional VA exchange or transfer services can be administrator-affiliated, non-affiliated, or a third-party provider. Providers of kiosks—often called "ATMs," bitcoin teller machines," "bitcoin ATMs," or "vending machines"—may also fall into the above definitions because they provide or actively facilitate

⁴ In this context of virtual assets, transfer means to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another.

⁵ In many jurisdictions, the term "exchange" is broad and can refer to both money transmission exchanges as well as to any organization, association, or group of persons, whether incorporated or unincorporated, that constitutes, maintains, or provides a market place or facilities for bringing together purchases and sellers or for otherwise performing (*e.g.*, with respect to securities) the functions commonly performed by a stock exchange as that term is generally understood and includes the market place and the market facilities maintained by the exchange.

- covered VA activities via physical electronic terminals (the kiosks) that enable the owner/operator to actively facilitate the exchange of VAs for fiat currency or other VAs.
38. Other VA services or business models may also constitute exchange or transfer activities based on items (i), (ii), and (iii) of the definition, and the natural or legal persons behind such services or models would therefore be VASPs if they conduct or facilitate the activity as a business on behalf of another person. These can include: VA escrow services, including services involving smart contract technology, that VA buyers use to send or transfer fiat currency in exchange for VAs, when the entity providing the service has custody over the funds; brokerage services that facilitate the issuance and trading of VAs on behalf of a natural or legal person's customers; order-book exchange services, which bring together orders for buyers and sellers,⁶ typically by enabling users to find counterparties, discover prices, and trade, potentially through the use of a matching engine that matches the buy and sell orders from users;⁷ and advanced trading services that allow users to buy portfolios of VAs and access more sophisticated trading techniques, such as trading on margin or algorithm-based trading.
 39. Peer-to-peer trading platforms are websites that enable buyers and sellers of VAs to find one another. Some trading platforms also facilitate trades as an intermediary. Depending on a jurisdiction's national legal framework, if a VA trading platform only provides a forum where buyers and sellers of VAs can post their bids and offers (with or without automatic interaction of orders), and the parties themselves trade at an outside venue (either through individual wallets or other wallets not hosted by the trading platform—*i.e.*, an individual user-to-individual user transaction), then the platform may not constitute a VASP as defined above. However, where the platform facilitates the exchange, transfer, or other financial activity involving VAs (as described in items (i) through (v), including by purchasing VAs from a seller when transactions or bids and offers are matched on the trading platform and selling the VAs to a buyer, then the platform is a VASP conducting exchange and/or transfer activity as a business on behalf of its customers.
 40. Exchange or transfer services may also occur through decentralized exchanges or platforms. "Decentralized (distributed) application (DApp)," for example, is a term that refers to software programs that operate on a peer-to-peer network of computers running a blockchain platform—a type of distributed public ledger that allows the development of secondary blockchains—designed such that they are not controlled by a single person or group of persons and thus do not have an identifiable administrator. An owner/operator of a DApp may deploy it to perform a wide variety of functions, including acting as an unincorporated organization,

⁶ Countries should assess the totality of activities and technology used to bring together orders of multiple buyers and sellers for securities using established non-discretionary methods under which such orders interact. A system brings together orders of buyers and sellers if, for example, it displays or otherwise represents trading interest entered on a system to users or if the system receives users' orders centrally for future processing and execution.

⁷ The example of an order-book exchange service provided here describes a typical "order book," which is usually a website interface that collects and displays orders for buyers and sellers and lets users find counterparties, discover prices, and trade through a matching engine. [EtherDelta \(U.S. Securities and Commission case, November 2018\)](#) is an example of an online platform that allowed buyers and sellers to trade Ether and ERC20 tokens in secondary market trading involving a VA order-book exchange service that provided a user interface with an order book to match trades and send them to be recorded on the distributed ledger. (In contrast, a peer-to-peer exchange platform is more akin to a bulletin board where one buyer and one seller might locate one another and then go to a different location to effect the trade between themselves.)

such as a software agency, to provide virtual asset activities.⁸ Generally, a DApp user must pay a fee to the DApp, which is commonly paid in VAs, for the ultimate benefit of the owner/operator in order to run the software. When DApps facilitate or conduct the exchange or transfer of value (whether in VA or traditional fiat currency), the DApp, its owner/operator(s), or both may fall under the definition of a VASP. Likewise, a person that develops a decentralized VA payment system may be a VASP when they engage as a business in facilitating or conducting the activities previously described on behalf of another natural or legal person.

41. In the context of item (iv) of the VASP definition, *safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets*, countries should account for services or business models that combine the function of safeguarding the value of a customer's VAs with the power to manage or transmit the VAs independently from the owner, under the assumption that such management and transmission will only be done according to the owner's/customer's instructions. Safekeeping and administration services include persons that have exclusive or independent control of the private key associated with VAs belonging to another person or exclusive and independent control of smart contracts to which they are not a party that involve VAs belonging to another person.
42. Natural or legal persons that actively facilitate the offer or issuance of and trading in VAs, including by accepting purchase orders and funds and purchasing VAs from an issuer to resell and distribute the funds or assets, may also fall within the scope of items (i), (ii), and (iii) as well as within item (v), participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.⁹ For example, ICOs are generally a means to raise funds for new projects from early backers and the natural and legal persons actively facilitating the issuance may provide services that involve exchange or transfer activity as well as issuance offer and/or sale activity.
43. A jurisdiction's applicable AML/CFT obligations governing service providers that participate in or provide financial services relating to an issuer's offer and/or sale, such as in the context of ICOs, may therefore involve both the jurisdiction's money transmission regulations as well as its regulations governing securities, commodities, or derivatives activities.
44. A VASP may fall into one or more of the five categories of activity or operation described under the VASP definition (*i.e.*, "exchange" of virtual/fiat, "exchange" of virtual/virtual, "transfer," "safekeeping and/or administration," and "participation in and provision of financial services related to an issuer's offer and/or sale").
45. For example, a number of online platforms that provide a mechanism for trading assets, including VAs offered and sold in ICOs, may meet the definition of an exchange and/or a security-related entity dealing in VAs that are "securities" under various jurisdictions' national legal frameworks. Other jurisdictions may have a different approach which may include payment tokens. The relevant competent authorities in jurisdictions should therefore strive to apply a functional approach that takes into account the relevant facts and circumstances of the platform, assets, and activity involved, among other factors, in determining whether the entity meets the definition of an "exchange" or other obliged entity (such as a securities-related entity) under their national legal framework and whether an entity falls within a particular

⁸ For an example of a DApp, see the U.S. Securities and Exchange Commission (SEC)'s Release No. 81207/ July 25, 2017, "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO," available at www.sec.gov/litigation/investreport/34-81207.pdf.

⁹ Activity (v). aims to cover similar activities, conducted in a VA context, as the ones described in Activity 8 of the FATF definition of Financial institutions "*Participation in securities issues and the provision of financial services related to such issues*" (*FATF Glossary*)

definition. In reaching a determination, countries and competent authorities should consider the activities and functions that the entity in question performs, regardless of the technology associated with the activity or used by the entity.

46. Whether a natural or legal person engaged in VA activities is a VASP depends on how the person uses the VA and for whose benefit. As emphasized above, if a person (natural or legal) is engaged as a business in any of the activities described in the FATF definition (*i.e.*, items (i) through (v)) for or on behalf of another person, then they are a VASP, regardless of what technology they use to conduct the covered VA activities. Moreover, they are a VASP, whether they use a decentralized or centralized platform, smart contract, or some other mechanism. However, a person not engaging as a business for or on behalf of another natural or legal person in the aforementioned activities (*e.g.*, an individual who obtains VAs and uses them to purchase goods or services on their own behalf or makes a one-off exchange or transfer) is not a VASP.
47. Just as the FATF does not seek to regulate the individual users (not acting as a business) of VAs as VASPs—though recognizing that such users may still be subject to compliance obligations under a jurisdiction’s sanctions or enforcement framework¹⁰—the FATF similarly does not seek to capture the types of closed-loop items that are non-transferable, non-exchangeable, and non-fungible. Such items might include airline miles, credit card awards, or similar loyalty program rewards or points, which an individual cannot sell onward in a secondary market. Rather, the VA and VASP definitions are intended to capture specific financial activities and functions (*i.e.*, transfer, exchange, safekeeping and administration, issuance, etc.) and assets that are fungible—whether virtual-to-virtual or virtual-to-fiat.
48. Likewise, the FATF does not seek to regulate the technology that underlies VAs or VASP activities, but rather the natural or legal persons behind such technology or software applications that may use technology or software applications to facilitate financial activity or conduct as a business the aforementioned VA activities on behalf of another natural or legal person. A person that develops or sells either a software application of a new VA platform (*i.e.*, a software developer) may therefore not constitute a VASP when solely developing or selling the application or platform, but they may be a VASP if they also use the new application or platform to engage as a business in exchanging or transferring funds or conducting any of the other financial activity described above on behalf of another natural or legal person. Further, the FATF does not seek to regulate as VASPs natural or legal persons that provide ancillary services or products to a virtual asset network, including hardware wallet manufacturers and non-custodial wallets, to the extent that they do not also engage in or facilitate as a business any of the aforementioned covered VA activities on behalf of their customers.
49. Importantly, in INR. 15, the FATF does not exempt specific assets based on terms that may lack a common understanding across jurisdictions or even among industry (*e.g.*, “utility tokens”), in part so that Recommendation 15 and its Interpretive Note may continue to be technology-neutral. Rather, the framing of the Recommendations, including Recommendation 15, is activity-based and focused on functions in order to provide jurisdictions with sufficient flexibility.
50. Flexibility is particularly relevant in the context of VAs and VA activities, which involve a range of products and services in a rapidly-evolving space. Some items—or tokens—that on their face do not appear to constitute VAs may in fact be VAs that enable the transfer or exchange of

¹⁰ In the United States, for example, such “users” must, like all U.S. persons or persons otherwise subject to U.S. jurisdiction, comply with all U.S. sanctions and regulations administered by the U.S. Department of the Treasury’s Office of Foreign Assets Control. Further, U.S. sanctions compliance obligations are the same, regardless of whether a transaction is denominated in digital currency or traditional fiat currency or involves some other form of asset or property.

value or facilitate ML/TF. Some ICOs, for example, relate to or involve “gaming tokens,” and other “gaming tokens” can be used to obfuscate transaction flows between an in-game token and its exchange for or transfer to a VA. Secondary markets also exist in both the securities and commodities sectors for “goods and services” that are fungible and transferable. For example, users can develop and purchase certain virtual items that act as a store of value and in fact accrue value or worth and that can be sold for value in the VA space.

51. As discussed above, countries should focus on the financial conduct or activity surrounding the VA or its underlying technology and how it poses ML/TF risks (*e.g.*, the potential for enhanced anonymity, obfuscation, disintermediation, and decreased transparency or technology, platforms, or VAs that undermine a VASP’s ability to perform AML or CDD) and apply measures accordingly.
52. Countries should address the ML/TF risks associated with VA activities, both where those activities intersect with the regulated fiat currency financial system, as appropriate under their national legal frameworks, which may offer various options for regulating such activity, as well as where such activities may not involve the fiat currency financial system but consist only of “virtual-to-virtual” interactions (*e.g.*, as in the case of exchanges between one or more forms of VA).
53. Similarly, AML/CFT regulations will apply to covered VA activities and VASPs, regardless of the type of VA involved in the financial activity (*e.g.*, a VASP that uses or offers AECs to its customers for various financial transactions), the underlying technology, or the additional services that the platform potentially incorporates (such as a mixer or tumbler or other potential features for obfuscation).
54. VASPs are subject to the relevant FATF measures that are similarly applicable to other entities subject to AML/CFT regulation under the FATF Recommendations, regardless of what a jurisdiction may term such providers, based on the types of activities in which VASPs engage. Further, as described in INR. 15, the measures applicable to “property,” “proceeds,” “funds,” “funds or assets,” and other “corresponding value” under the FATF Recommendations also apply to VAs (*e.g.*, Recommendations 3 – 8, 30, 33, 35, and 38).

SECTION III – APPLICATION OF FATF STANDARDS TO COUNTRIES AND COMPETENT AUTHORITIES

55. Section III explains how the FATF Recommendations relating to VAs and VASPs apply to countries and competent authorities and focuses on identifying and mitigating the risks associated with covered VA activities, applying preventive measures, applying licensing and registration requirements, implementing effective supervision on par with the supervision of related financial activities of FIs, providing a range of effective and dissuasive sanctions, and facilitating national and international co-operation. Almost all of the FATF Recommendations are directly relevant for understanding how countries should use government authorities and international co-operation to address the ML/TF risks associated with VAs and VASPs, while other Recommendations are less directly or explicitly linked to VAs or VASPs, though are still relevant and applicable.
56. VAs and VASPs are subject to the full range of obligations under the FATF Recommendations, as described in INR. 15, including those obligations applicable to other entities subject to AML/CFT regulation, based on the financial activities in which VASPs engage and having regard to the ML/TF risks associated with covered VA activities or operations.
57. This section also reviews the application of the risk-based approach by supervisors of VASPs.

Application of the Recommendations in the Context of VAs and VASPs

Risk-Based Approach and National Co-ordination

58. **Recommendation 1.** The FATF Recommendations make clear that countries should apply a risk-based approach to ensure that measures to prevent or mitigate ML/TF risks are commensurate with the risks identified in their respective jurisdictions. Under the risk-based approach, countries should strengthen the requirements for higher-risk situations or activities involving VAs. When assessing the ML/TF risks associated with VAs, the particular types of VA financial activities, and the activities or operations of VASPs, the distinction between centralized and decentralized VAs, as discussed in the 2015 VC Guidance, will likely continue to be a key aspect for countries to consider. Due to the potential for increased anonymity or obfuscation of VA financial flows and the challenges associated with conducting effective customer identification and verification, VAs and VASPs in general may be regarded as higher ML/TF risks that may potentially require the application of enhanced due diligence measures, where appropriate.
59. Recommendation 1 requires countries to identify, understand, and assess their ML/TF risks and to take action aimed at effectively mitigating those risks. The requirement applies in relation to the risks associated with new technologies under Recommendation 15, including VAs and the risks associated with VASPs that engage in or provide covered VA activities, operations, products, or services. Public-private sector co-operation may assist competent authorities in developing AML/CFT policies for covered VA activities (*e.g.*, VA payments, VA transfers, VA issuance, etc.) as well as for innovations in related VA technologies and emerging products and services, where appropriate and applicable. Co-operation may also assist countries in allocating and prioritizing AML/CFT resources by competent authorities.
60. National authorities should undertake a co-ordinated risk assessment of VA activities, products, and services, as well as of the risks associated with VASPs and the overall VASP sector in their country, if any. The risk assessment should (i) enable all relevant authorities to understand how specific VA products and services function, fit into, and affect all relevant regulatory jurisdictions for AML/CFT purposes (*e.g.*, money transmission and payment mechanisms, VA kiosks, VA commodities, VA securities or related issuance activities, etc., as

- highlighted in the VASP definition) and (ii) promote similar AML/CFT treatment for similar products and services with similar risk profiles.
61. As the VASP sector evolves, countries should consider examining the relationship between AML/CFT measures for covered VA activities and other regulatory and supervisory measures (e.g., consumer protection, prudential safety and soundness, network IT security, tax, etc.), as the measures taken in other fields may affect the ML/TF risks. In this regard, countries should consider undertaking short- and longer-term policy work to develop comprehensive regulatory and supervisory frameworks for covered VA activities and VASPs (as well as other obliged entities operating in the VA space) as widespread adoption of VAs continues.
 62. Countries should also require VASPs (as well as other obliged entities) to identify, assess, and take effective action to mitigate the ML/TF risks associated with providing or engaging in covered VA activities or associated with offering particular VA products or services. Where VASPs are permitted under national law, countries, VASPs, as well as FIs and DNFBPs—including FIs or DNFBPs that engage in VA activities or provide VA products or services—must assess the associated ML/TF risks and apply a risk-based approach to ensure that appropriate measures to prevent or mitigate those risks are implemented.
 63. A jurisdiction has the discretion to prohibit VA activities or VASPs, based on their assessment of risk and national regulatory context or in order to support other policy goals not addressed in this Guidance (e.g., consumer protection, safety and soundness, or monetary policy). Where countries consider prohibiting VA activities or VASPs, they should take into account the effect that such a prohibition may have on their ML/TF risks. Regardless of whether a country opts to prohibit or regulate the sector, additional measures may be useful in mitigating the overall ML/TF risks. For example, if a country prohibits VA activities and VASPs, mitigation measures should include identifying VASPs (or other obliged entities that may engage in VA activities) that operate illegally in the jurisdiction and applying proportionate and dissuasive sanctions to such entities. Based on the country's risk profile, prohibition should still require outreach and enforcement actions by the country as well as risk mitigation strategies that account for the cross-border element of VA activities (e.g., cross-border VA payments or transfers) and VASP operations.
 64. **Recommendation 2** requires national co-operation and co-ordination with respect to AML/CFT policies, including in the VASP sector, and is therefore indirectly applicable to countries in the context of regulating and supervising covered VA activities. Countries should consider putting in place mechanisms, such as interagency working groups or task forces, to enable policymakers, regulators, supervisors, the financial intelligence unit (FIU), and law enforcement authorities to co-operate with one another and any other relevant competent authorities in order to develop and implement effective policies, regulations, and other measures to address the ML/TF risks associated with covered VA activities and VASPs. This should include co-operation and co-ordination between relevant authorities to ensure the compatibility of AML/CFT requirements with Data Protection and Privacy rules and other similar provisions (e.g., data security/localisation). National co-operation and co-ordination are particularly important in the context of VAs, in part due to their highly-mobile and cross-border nature and because of the manner in which covered or regulated VA activities may implicate multiple regulatory bodies (e.g., those competent authorities regulating money transmission, securities, and commodities or derivatives activities). Further, national co-operation relating to VA issues is vital in the context of furthering investigations and leveraging various interagency tools relevant for addressing the cyber and/or VA ecosystem.

Treatment of Virtual Assets: Interpreting the Funds- or Value-Based Terms

65. For the purposes of applying the FATF Recommendations, countries should consider all funds- or value-based terms in the Recommendations, such as “property,” “proceeds,” “funds,” “funds

or other assets,” and other “corresponding value,” as including VAs. In particular, countries should apply the relevant measures under Recommendations 3 through 8, 30, 33, 35, and 38, all of which contain references to the aforementioned funds- or value-based terms or other similar terms, in the context of VAs in order to prevent the misuse of VAs in ML, TF, and proliferation financing (PF) and take action against all proceeds of crime involving VAs. The aforementioned Recommendations—some of which may not at first appear directly applicable to VASPs and similarly obliged entities but are in fact applicable in this space—relate to the ML offence, confiscation and provisional measures, TF offence, targeted financial sanctions, non-profit organisations, law enforcement powers, sanctions, and international co-operation.

66. **Recommendation 3.** For the purposes of implementing Recommendation 3, the ML offence should extend to any type of property, regardless of its value, that directly represents the proceeds of crime, including in the context of VAs. When proving that property is the proceeds of crime, it should not be necessary that a person be convicted of a predicate offence, including in the case of VA-related proceeds. Countries should therefore extend their applicable ML offence measures to proceeds of crime involving VAs.
67. **Recommendation 4.** Similarly, the confiscation and provisional measures relating to “(a) property laundered, (b) proceeds from, or instrumentalities used in or intended for use in money laundering or predicate offences, (c) property that is used in, or intended or allocated for use in, the financing of terrorism, terrorist acts, or terrorist organisations, (d) or property of corresponding value” also apply to VAs.
68. As for confiscation or temporary measures applicable to fiat currencies and goods, law enforcement authorities (LEAs) should be able to request a temporary freeze of assets when there are grounds to establish or when it is established, that they originate from criminal activity. To extend the duration of the freeze or to request the confiscation of assets, LEAs should obtain a court order.
69. **Recommendation 5.** Likewise, the TF offences described in Recommendation 5 should extend to “any funds or other assets,” including VAs, whether from a legitimate or illegitimate source (see INR. 5).
70. **Recommendation 6.** Countries should also freeze without delay the funds or other assets—including VAs—of designated persons or entities and ensure that no funds or other assets—including VAs—are made available to or for the benefit of designated persons or entities in relation to the targeted financial sanctions related to terrorism and terrorist financing.
71. **Recommendation 7.** In the context of targeted financial sanctions related to proliferation, countries should freeze without delay the funds or other assets—including VAs—of designated persons or entities and ensure that no funds or others assets—including VAs—are made available to or for the benefit of designated persons or entities.
72. **Recommendation 8.** Countries also should apply measures, in line with the risk-based approach, to protect non-profit organisations from terrorist financing abuse, as laid out in Recommendation 8, including when the clandestine diversion of funds to terrorist organisations involves VAs (see Recommendation 8(c)).
73. **Recommendation 30** applies to covered VA activities and VASPs in the context of the applicability of all funds- or value-based terms addressed in sub-section 3.1.2 of this Guidance. As with other types of property or proceeds of crime, countries should ensure that competent authorities have responsibility for expeditiously identifying, tracing, and initiating actions to freeze and seize VA- related property that is, or may become, subject to confiscation or is suspected of being the proceeds of crime. Countries should implement Recommendation 30, regardless of how the jurisdiction classifies VAs in its national legal framework (*i.e.*, regardless of how VAs are categorized legally with respect to the property laws of the jurisdiction).

74. **Recommendation 33.** The statistics that countries maintain should include statistics on the suspicious transaction reports (STRs) that the competent authorities receive and disseminate as well as on the property that the competent authorities freeze, seize, and confiscate. Countries should therefore also implement Recommendation 33 in the context of VASPs and VA activities and maintain statistics on the STRs that competent authorities receive from VASPs and from other obliged entities, such as banks, that submit STRs relating to VASPs, VAs, or VA activities. As with other Recommendations that contain funds- or value-based terms (e.g., Recommendation 3 through 8, 30, 35, and 38), countries should also maintain statistics on any VAs that competent authorities freeze, seize, or confiscate, regardless of how the jurisdiction categorizes VAs with respect to the property laws of its national legal framework. Additionally, countries should consider updating their STRs and associated statistics to incorporate VA-related indicators that facilitate investigations and financial analysis.
75. **Recommendation 35** directs countries to have a range of effective, proportionate and dissuasive sanctions (criminal, civil or administrative) available to deal with natural or legal persons covered by Recommendations 6 and 8 to 23 that fail to comply with the applicable AML/CFT requirements. As required by paragraph 6 of INR. 15, countries should similarly have in place sanctions to deal with VASPs (and other obliged entities that engage in VA activities) that fail to comply with their AML/CFT requirements. As with FIs and DNFBPs and other natural or legal persons, such sanctions should be applicable not only to VASPs but also to their directors and senior management, where applicable.
76. **Recommendation 38** also contains funds- or value-based terms and applies in the context of VAs but is addressed in further detail in sub-section 3.1.8 on *International Co-operation* and the implementation of Recommendations 37 through 40, as described in paragraph 8 of INR. 15.

Licensing or Registration

77. Countries should designate one or more authorities that have responsibility for licensing and/or registering VASPs.
78. In accordance with INR. 15 paragraph 3, at a minimum, VASPs should be required to be licensed or registered in the jurisdiction(s) where they are created. References to creating a legal person¹¹ include the incorporation of companies or any other mechanism that is used domestically to formalise the existence of a legal entity, such as registration in the public register, commercial register, or any equivalent register of companies or legal entities; recognition by a notary or any other public officer; filing of the company bylaws or articles of incorporation; allocation of a company tax number, etc.
79. In cases where the VASP is a natural person, it should be required to be licensed or registered in the jurisdiction where its place of business is located—the determination of which may include several factors for consideration by countries. The place of business of a natural person can be characterised by the primary location where the business is performed or where the business' books and records are kept as well as where the natural person resides (i.e., where the natural person is physically present, located, or resident). When a natural person conducts business from his/her residence, or a place of business cannot be identified, his/her primary residence may be regarded as his/her place of business, for example. The place of business may also include, as a potential factor for consideration, the location of the server of the business.
80. VASPs that are licensed or registered should be required to meet appropriate licensing and registration criteria set by relevant authorities. Authorities should impose such conditions on licenced or registered VASPs to be able to effectively supervise the VASPs. Such conditions

¹¹ See footnote 40 in INR. 24.

- should allow for sufficient supervisory hold and could potentially include, depending on the size and nature of the VASP activities, requiring a resident executive director, substantive management presence, or specific financial requirements.
81. Jurisdictions may also require VASPs that offer products and/or services to customers in, or that conduct operations from, their jurisdiction to be licensed or registered in the jurisdiction. Host jurisdictions may therefore require registration or licencing of VASPs whose services can be accessed by or are made available to people residing or living within their jurisdiction.
 82. Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a VASP. Such measures should include requiring VASPs to seek authorities' prior approval for substantive changes in shareholders, business operations, and structures.
 83. Countries should take action to identify natural or legal persons that carry out VA activities or operations without the requisite license or registration and apply appropriate sanctions, including in the context of traditional obliged entities that may engage in VA activities or operations (*e.g.*, a bank that provides VAs to its customers). National authorities should have mechanisms to monitor the VASP sector as well as other obliged entities that may engage in covered VA activities or operations or provide covered VA products or services and ensure that appropriate channels are in place for informing VASPs and other obliged entities of their obligation to register or apply for a license with the relevant authority. Countries should also designate an authority responsible for identifying and sanctioning unlicensed or unregistered VASPs (as well as other obliged entities that engage in VA activities). As discussed above in the Guidance, even countries that choose to prohibit VA activities or VASPs in their jurisdiction should have in place tools and authorities to identify and take action against natural or legal persons that fail to comply with their legal obligations, as required under Recommendation 15.
 84. In order to identify persons operating without a license and/or registration, countries should consider the range of tools and resources they may have for investigating the presence of an unlicensed or unregistered VASP. For example, countries should consider web-scraping and open-source information to identify online advertising or possible solicitations for business by an unregistered or unlicensed entity; information from industry circles (including by establishing channels for receiving public feedback) regarding the presence of certain businesses that may be unlicensed or unregistered; FIU or other information from reporting institutions, such as STRs or bank-provided investigative leads that may reveal the presence of an unlicensed or unregistered natural or legal person VASP; non-publically available information, such as whether the entity previously applied for a license or registration or had its license or registration withdrawn and law enforcement and intelligence reports; as well as other investigative tools or capabilities.
 85. Co-ordination between various national authorities involved in the regulation and licensing or registration of VASPs is important, as described previously in the context of Recommendation 2, since various authorities may hold information relating to unauthorised providers or activities. Countries should have in place relevant channels for sharing information as appropriate to support the identification and sanctioning of unlicensed or unregistered VASPs.

Supervision or Monitoring

86. **Recommendations 26 and 27.** As discussed below, Recommendation 15 requires countries to subject VASPs to effective systems for AML/CFT supervision or monitoring. As set forth in Recommendation 26 and 27, paragraph 5 of INR. 15 similarly requires countries to ensure that VASPs are also subject to adequate regulation and supervision or monitoring for AML/CFT and are effectively implementing the FATF Recommendations, in line with their ML/TF risks.

VASPs should be subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements. VASPs should be supervised or monitored by a competent authority, not a self-regulatory body (SRB), which should conduct risk-based supervision or monitoring. Supervisors should have adequate powers to supervise or monitor and ensure compliance by VASPs (as well as other obliged entities that engage in VA activities) with requirements to combat money laundering and terrorist financing including the authority to conduct inspections, compel the production of information, and impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict, or suspend the VASP's license or registration, where applicable.

87. Given the cross-border nature of VASPs' activities and provision of services and the potential challenges in associating a particular VASP with a single jurisdiction, international co-operation between relevant supervisors is also of specific importance, as underlined in paragraph 8 of INR. 15 (see also sub-section 3.1.8). Jurisdictions could also refer to the relevant work of other international standard-setting bodies for useful guidance in this respect, such as the International Organization of Securities Commissions as well as the Basel Committee on Banking Supervision.¹²
88. As discussed in more detail in sub-section 3.1.9 of this Guidance, when a DNFBP engages in VASP activity, countries should subject the entity to all of the relevant measures for VASPs set forth in the FATF Recommendations, including with respect to supervision or monitoring.¹³

Preventive Measures

89. Paragraph 7 of INR. 15 makes clear that all of the preventive measures contained in Recommendations 10 through 21 apply to both countries and obliged entities in the context of VAs and VA financial activities. However, Recommendations 9, 22, and 23 also have indirect applicability in this space and are discussed below as well. Accordingly, the following sub-section provides a Recommendation-by-Recommendation explanation to help countries in further considering how to implement the preventive measures in the context of VAs. Relatedly, sub-section 4.1 provides guidance specific to VASPs and other obliged entities that engage in VA activities on how they should implement the preventive measures described below as well as other AML/CFT measures throughout the FATF Recommendations.
90. **Recommendation 9** is intended to ensure that financial institution secrecy laws do not inhibit the implementation of the FATF Recommendations. As with FIs, countries should similarly ensure that secrecy laws do not inhibit the implementation of the FATF Recommendations to VASPs, although Recommendation 9 does not explicitly include or mention VASPs.
91. **Recommendation 10.** Countries and obliged entities should design CDD processes to meet the FATF Standards and national legal requirements. The CDD process should help VASPs (as well as other obliged entities that engage in VA activities) in assessing the ML/TF risks associated with covered VA activities or business relationships or occasional transactions above the threshold. Initial CDD comprises identifying the customer and, where applicable, the customer's beneficial owner and verifying the customer's identity on a risk basis and on the basis of reliable and independent information, data, or documentation to at least the extent

¹² See, for example, Principles 3 (on co-operation and collaboration) and 13 (on home-host relationships) of the Committee's *Core Principles for Effective Banking Supervision*: www.bis.org/publ/bcbs230.pdf.

¹³ As outlined in sub-section 2.2, jurisdictions may call or term VASPs as "FIs" or as "DNFBPs." However, regardless of what countries may choose to call VASPs, they are still subject to the same level of regulation and supervision as FIs, in line with the types of financial activities in which VASPs engage and the types of financial services they provide.

required by the applicable legal or regulatory framework. The CDD process also includes understanding the purpose and intended nature of the business relationship, where relevant, and obtaining further information in higher risk situations.

92. In practice, VASPs typically open and maintain accounts (*i.e.*, establish a customer relationship) and collect the relevant CDD information when they provide services to or engage in covered VA activities on behalf of their customers. In cases where a VASP carries out an occasional transaction, however, the designated threshold above which VASPs are required to conduct CDD is USD/EUR 1 000, in accordance with INR. 15, paragraph 7(a).¹⁴
93. Regardless of the nature of the relationship or transaction, countries should ensure that VASPs have in place effective procedures to identify and verify, on a risk basis, the identity of a customer, including when establishing business relations with that customer; where VASPs may have suspicions of ML/TF, regardless of any exemption of thresholds; and where they have doubts about the veracity or adequacy of previously obtained identification data.
94. Some jurisdictions may consider the use of VA kiosks (which some may refer to as VA “ATMs,” as described in the section above on VA services and business models) as an occasional transaction, whereby the provider or owner/operator of the kiosk and the customer using the kiosk transact on a one-off basis. Other jurisdictions may require owners/operators of such kiosks (*i.e.*, the kiosk provider) to register as a VASP or other financial institution (*e.g.*, as a money transmitters) and may not consider such transactions to be occasional.
95. As discussed previously, VAs have certain characteristics that may make them more susceptible to abuse by criminals, money launderers, terrorist financiers, and other illicit actors, including their global reach, capacity for rapid settlement, ability to enable “individual user-to-individual user” transactions (sometimes referred to as “peer-to-peer”), and potential for increased anonymity and obfuscation of transaction flows and counterparties. In light of these characteristics, countries may therefore go further than what Recommendation 10 requires by requiring full CDD for all transactions involving VAs or performed by VASPs (as well as other obliged entities, such as banks that engage in VA activities), including “occasional transactions” below the USD/EUR 1 000 threshold, in line with their national legal frameworks. Such an approach is consistent with the risk-based approach set out in Recommendation 1, provided that it is justified on the basis of the country’s assessment of risks (*e.g.*, through the identification of higher risks). Additionally, jurisdictions, in establishing their regulatory and supervisory regimes, should consider how the VASP can determine and ensure that the transactions are in fact only conducted on a one-off or occasional basis rather than a more consistent (*i.e.*, non-occasional) basis.
96. As described in the Interpretive Note to Recommendation 10, there are circumstances where the ML/TF risk is higher and where enhanced CDD measures must be taken. In the context of VA-related activities and VASPs, for example, countries should consider country- or geographic-specific risk factors. VASPs located in or VA transfers from or associated with particular countries present potentially higher risks for money laundering or terrorist financing (see INR. 10, paragraph 15(b)).
97. While there is no universally agreed upon definition or methodology for determining whether a jurisdiction, in which a VASP operates or from which VA transactions may emanate, represents a higher risk for ML/TF, the consideration of country-specific risks, in conjunction with other risk factors, provides useful information for further determining potential ML/TF risks. Indicators of higher risk include:

¹⁴ The FATF agreed to lower the threshold amount for VA-related transactions to USD/EUR 1 000, given the ML/TF risks associated with and cross-border nature of VA activities.

- a) Countries or geographic areas identified by credible sources¹⁵ as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them;
 - b) Countries identified by credible sources as having significant levels of organized crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking, smuggling, and illegal gambling;
 - c) Countries that are subject to sanctions, embargoes, or similar measures issued by international organisations such as the United Nations; and
 - d) Countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by the FATF statements as having weak AML/CFT regimes, and for which financial institutions should give special attention to business relationships and transactions.
98. Countries also should consider the risk factors associated with the VA product, service, transaction, or delivery channel, including whether the activity involves pseudonymous or “anonymous transactions,” “non-face-to-face business relationships or transactions,” and/or “payment[s] received from unknown or un-associated third parties” (see INR. 10 15(c) as well as the examples of higher and lower risk indicators listed in paragraph 31 of this Guidance). The fact that nearly all VAs include one or more of these features or characteristics may result in countries determining that activities in this space are inherently higher risk, based on the very nature of VA products, services, transactions, or delivery mechanisms.
99. In these and other cases, the enhanced due diligence (EDD) measures that may mitigate the potentially higher risks associated with the aforementioned factors include:
- a) corroborating the identity information received from the customer, such as a national identity number, with information in third-party databases or other reliable sources;
 - b) potentially tracing the customer’s IP address; and
 - c) searching the Internet for corroborating activity information consistent with the customer’s transaction profile, provided that the data collection is in line with national privacy legislation.¹⁶
100. Countries also should consider the enhanced CDD measures detailed in INR. 10, paragraph 20, including obtaining additional information on the customer and intended nature of the business relationship, obtaining information on the source of funds of the customer, obtaining information on the reasons for intended or performed transactions, and conducting enhanced monitoring of the relationship. Additionally, countries should consider the measures required for FIs that engage in fiat-denominated activity that is non-face-to-face (such as mobile

¹⁵ “Credible sources” refers to information that is produced by reputable and universally recognised international organisations and other bodies that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, the World Bank, and the Egmont Group of Financial Intelligence Units.

¹⁶ See 2015 VC Guidance, paragraph 44 as well as June 2013 Guidance for a Risk-Based Approach to New Payment Products and Services, paragraph 66.

- services) or that is comparable to VA transactions in assessing their risks and developing mitigating controls accordingly.
101. Additionally, countries should require VASPs and other obliged entities that engage in or provide VA products and services to keep documents, data, or information collected under the CDD process up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk customers or categories of VA products or services, and conducting ongoing due diligence (see Section IV for further discussion on ongoing due diligence and monitoring obligations for VASPs and other obliged entities). Such transactional and record reviews are vital for effective supervision.
 102. **Recommendation 11** requires countries to ensure that VASPs maintain all records of transactions and CDD measures for at least five years in such a way that individual transactions can be reconstructed and the relevant elements provided swiftly to competent authorities. Countries should require VASPs and other obliged entities engaging in VA activities to maintain transaction records on transactions and information obtained through CDD measures, including: information relating to the identification of the relevant parties, the public keys (or equivalent identifiers), addresses or accounts involved (or equivalent identifiers), the nature and date of the transaction, and the amount transferred, for example. The public information on the blockchain or other relevant distributed ledger of a particular VA may provide a beginning foundation for recordkeeping, provided institutions can adequately identify their customers. However, reliance solely on the blockchain or other type of distributed ledger underlying the VA for recordkeeping is not sufficient for compliance with Recommendation 11.
 103. For example, the information available on the blockchain or other type of distributed ledger may enable relevant authorities to trace transactions back to a wallet address, though may not readily link the wallet address to the name of an individual. The wallet address contains a user code that serves as a digital signature in the distributed ledger (*i.e.*, a private key) in the form of a unique string of numbers and letters. However, additional information will be necessary to associate the address to a real or natural person.
 104. **Recommendation 12** requires countries to implement measures requiring obliged entities such as VASPs to have appropriate risk management systems in place to determine whether customers or beneficial owners are foreign politically exposed persons (PEPs)¹⁷ or related or connected to a foreign PEP and, if so, to take additional measures beyond performing normal CDD (as defined in Recommendation 10) to determine if and when they are doing business with them, including identifying the source of funds when relevant.
 105. **Recommendation 13** stipulates that countries should require FIs to apply certain other obligations in addition to performing normal CDD measures when they engage in cross-border correspondent relationships. Separate and apart from traditional FIs that may engage in covered VA activities and for which all of the measures of Recommendation 13 already apply, some other business relationships or covered VA activities in the VASP sector may have characteristics similar to cross-border correspondent banking relationships. INR. 13 stipulates that for correspondent banking and other similar cross-border relationships, FIs should apply criteria (a) to (e) of Recommendation 13, in addition to performing normal CDD measures. “Other similar relationships” includes money or value transfer services (MVTS) when MVTS providers act as intermediaries for other MVTS providers or where an MVTS provider accesses

¹⁷ “Foreign PEPs” are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, and important political party officials (FATF Glossary).

- banking or similar services through the account of another MVTS customer of the bank (see *2016 FATF Guidance on Correspondent Banking Relationships*).
106. To the extent that relationships in the VASP sector currently have or may in the future¹⁸ have characteristics similar to cross-border correspondent banking relationships, countries should implement the preventive measures set forth in Recommendation 13 to VASPs (and other obliged entities operating in the VA space) that develop such relationships.
 107. **Recommendation 14** directs countries to register or license natural or legal persons that provide MVTS in the country and ensure their compliance with the relevant AML/CFT measures. As described in the 2015 VC Guidance, this includes subjecting MVTS operating in the country to monitoring for compliance with registration or licensing and other applicable AML/CFT measures. The registration and licensing requirements of Recommendation 15, however, apply to all VASPs, even those engaging in MVTS activities (*e.g.*, domestic entities that provide as a business convertible VA exchange services between virtual and fiat currencies in a jurisdiction).
 108. **Recommendation 15.** In October 2018, the FATF adopted updates to Recommendation 15, which reinforce the fundamental risk-based approach and related obligations for countries and obliged entities in the context of new technologies, in order to clarify its application in the context of VAs, covered VA financial activities, and VASPs. Recommendation 15 requires countries to identify and assess the ML/TF risks relating to the development of new products and business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Notably, it also requires countries to ensure that financial institutions licensed by or operating in their jurisdiction take appropriate measures to manage and mitigate the associated ML/TF risks before launching new products or business practices or using new or developing technologies (see Annex A).
 109. In line with the spirit of Recommendation 15, the October 2018 update further clarifies that countries should manage and mitigate the risks emerging from VAs and ensure that VASPs are regulated for AML/CFT purposes, licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. INR. 15, which the FATF adopted in June 2019, further clarifies Recommendation 15 and defines more specifically how the FATF requirements apply in relation to VAs, covered VA activities, and VASPs, including in the context of: assessing the associated ML/TF risks; licensing or registration; supervision or monitoring; preventive measures such as CDD, recordkeeping, and suspicious transaction reporting, among others; sanctions and other enforcement measures; and international co-operation (see Annex A).
 110. In the context of VA and VASP activities, countries should ensure that VASPs licensed by or operating in their jurisdiction consider whether the VASP can manage and mitigate the risks of engaging in activities that involve the use of anonymity-enhancing technologies or mechanisms, including but not limited to AECs, mixers, tumblers, and other technologies that obfuscate the identity of the sender, recipient, holder, or beneficial owner of a VA. If the VASP cannot manage and mitigate the risks posed by engaging in such activities, then the VASP should not be permitted to engage in such activities.
 111. **Recommendation 16** was developed with the objective of preventing terrorists and other criminals from having unfettered access to electronically-facilitated funds transfers—which at the time of drafting the FATF termed “wire transfers”—for moving their funds and for detecting such misuse when it occurs. It establishes the requirements for countries relating to

¹⁸ For example, a number of researchers and analysts have indicated that they see great potential for VASPs and VA protocols to connect directly to existing correspondent banking customers and enable them to send and receive funds across borders, without the intermediation of traditional FIs, potentially leading to quicker settlements and reductions in cost.

wire transfers and related messages and applies to both domestic and cross-border wire transfers. Recommendation 16 defines “wire transfers” as any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.

112. In accordance with the functional approach of the FATF Recommendations, the requirements relating to wire transfers and related messages under Recommendation 16 apply to all providers of such services, including VASPs that provide services or engage in activities, such as VA transfers, that are functionally analogous to wire transfers. Countries should apply Recommendation 16 regardless of whether the value of the traditional wire transfer or the VA transfer is denominated in fiat currency or a VA. However, countries may adopt a *de minimis* threshold for VA transfers of USD/EUR 1 000, having regard to the risks associated with various VAs and covered VA activities.
113. Consequently, the requirements of Recommendation 16 should apply to VASPs whenever their transactions, whether in fiat currency or VA, involve: (a) a traditional wire transfer, or (b) a VA transfer or other related message operation between a VASP and another obliged entity (*e.g.*, between two VASPs or between a VASP and another obliged entity, such as a bank or other FI). In the latter scenarios (*i.e.*, transactions involving VA transfers), countries should treat all VA transfers as cross-border wire transfers, in accordance with the Interpretative Note to Recommendation 16 (INR. 16), rather than domestic wire transfers, based on the cross-border nature of VA activities and VASP operations.
114. As described in INR.15, paragraph 7(b), all of the requirements set forth in Recommendation 16 apply to VASPs or other obliged entities that engage in VA transfers, including the obligations to obtain, hold, and transmit required originator and beneficiary information in order to identify and report suspicious transactions, monitor the availability of information, take freezing actions, and prohibit transactions with designated persons and entities. Countries should therefore ensure that ordering institutions (whether a VASP or other obliged entity such as a FI) involved in a VA transfer obtain and hold required and accurate¹⁹ originator information and required beneficiary information and submit the information to beneficiary institutions (whether a VASP or other obliged entity such as a FI), if any. Further, countries should ensure that beneficiary institutions (whether a VASP or other obliged entity) obtain and hold required (not necessarily accurate) originator information and required and accurate beneficiary information, as set forth in INR. 16. The required information includes the: (i) originator’s name (*i.e.*, the sending customer); (ii) originator’s account number where such an account is used to process the transaction (*e.g.*, the VA wallet); (iii) originator’s physical (geographical) address, or national identity number, or customer identification number (*i.e.*, not a transaction number) that uniquely identifies the originator to the ordering institution, or date and place of birth; (iv) beneficiary’s name; and (v) beneficiary account number where such an account is used to process the transaction (*e.g.*, the VA wallet). It is not necessary for the information to be attached directly to the VA transfer itself. The information can be submitted either directly or indirectly, as set forth in INR. 15.
115. It is vital that countries ensure that providers of VA transfers—whether VASPs or other obliged entities—transmit the required originator and beneficiary information *immediately* and *securely*, particularly given the rapid and cross-border nature of VA transfers and in line with the objectives of Recommendation 16 (as well as the traditional requirement in Recommendation 16 for originator and beneficiary information to “accompany [...] wire transfers” involving fiat currency). “*Securely*” in the context of INR. 15, paragraph 7(b), is meant to convey that providers should protect the integrity and availability of the required

¹⁹ See FATF Glossary of specific terms used in Recommendation 16, wherein “accurate is used to describe information that has been verified for accuracy”.

information to facilitate recordkeeping (among other requirements) and the use of such information by receiving VASPs or other obliged entities as well as to protect it from unauthorized disclosure. Use of the term is not meant to impede the objectives of Recommendation 16 or Recommendation 9. “Immediately,”—also in the context of INR. 15, paragraph 7(b) and given the cross-border nature, global reach, and transaction speed of VAs—means that providers should submit the required information simultaneously or concurrently with the transfer itself. (See Section IV for additional information on these issues specific to VASPs and other obliged entities.)

116. Countries should require both the ordering and beneficiary institution under their national frameworks to make the above required information available to appropriate authorities upon request. Further, they should require both ordering and beneficiary institutions to take freezing actions and prohibit transactions with designated persons and entities (*i.e.*, screening customers in order to comply with their targeted financial sanctions obligations). Accordingly, the ordering institution should have the required information about its customer, the originator, and the beneficiary institution should have the required information about its customer, the beneficiary, in line with the customer due diligence requirements set forth in Recommendation 10.
117. The FATF recognizes that unlike traditional fiat wire transfers, not every VA transfer may involve (or be bookended by) two obliged entities, whether a VASP or other obliged entity such as a FI. In instances in which a VA transfer involves only one obliged entity on either end of the transfer (*e.g.*, when an ordering VASP or other obliged entity sends VAs on behalf of its customer, the originator, to a beneficiary that is not a customer of a beneficiary institution but rather an individual VA user who receives the VA transfer using his/her own distributed ledger technology (DLT) software, such as an unhosted wallet), countries should still ensure that the obliged entity adheres to the requirements of Recommendation 16 with respect to their customer (the originator or the beneficiary, as the case may be). The FATF does not expect that VASPs and financial institutions, when originating a VA transfer, would submit the required information to individual users who are not obliged entities. VASPs receiving a VA transfer from an entity that is not a VASP or other obliged entity (*e.g.*, from an individual VA user using his/her own DLT software, such as an unhosted wallet), should obtain the required originator information from their customer.
118. Similarly, there may be VA transfer scenarios, either now or in the near-future, that involve “intermediary VASPs” or other intermediary obliged entities or FIs that facilitate VA transfers as an intermediate element in a chain of VA transfers. Countries should ensure that such intermediary institutions (whether a VASP or other obliged entity) also comply with the requirements of Recommendation 16, as set forth in INR. 15, including the treatment of all VA transfers as cross-border qualifying transfers. Just as a traditional intermediary FI processing a traditional fiat cross-border wire transfer must ensure that all required originator and beneficiary information that accompanies a wire transfer is retained with it, so too must an intermediary VASP or other comparable intermediary institution that facilitates VA transfers ensure that the required information is transmitted along the chain of VA transfers as well as to maintain necessary records and make the information available to appropriate authorities upon request. Intermediary institutions involved in VA transfers also have obligations under Recommendation 16 to identify suspicious transactions, take freezing actions, and prohibit transactions with designated persons and entities—just like ordering and beneficiary VASPs (or other ordering or beneficiary obliged entities that facilitate VA transfers).
119. Consistent with the FATF’s technology-neutral approach, the required information need not be communicated as part of (or incorporated into) the transfer on the blockchain or other distributed ledger platform itself. Submitting information to the beneficiary VASP could be an entirely distinct process from that of the blockchain or other distributed ledger VA transfer. Any technology or software solution is acceptable, provided that the solution enables the

- ordering and beneficiary institutions to comply with the requirements of Recommendation 16 (and does not, of course, impede their ability to comply with their other AML/CFT obligations under the FATF Recommendations). Countries should engage with their private sectors on potential applications of available technology or possible solutions for compliance with Recommendation 16 (see Section IV for additional detail specific to providers and other obliged entities in the context of Recommendation 16).
120. **Recommendation 17** allows countries to permit obliged entities to rely on third parties to introduce business and/or perform part of the CDD process, including the identification and verification of customers' identities. The third party, however, must be a regulated entity that the competent authorities supervise and monitor for AML/CFT, with measures in place for compliance with CDD and recordkeeping requirements.
 121. Countries may permit VASPs to act as third parties, in accordance with their status under Recommendation 15. In addition to checking the regulated status of the third party, obliged entities should conduct their selection on a risk basis. In the context of third-party VASPs, countries and obliged entities should consider the risks potentially posed by the third party, the nature of the business or operation, the third-party VASP's customer groups or target markets, and its business partners, where relevant. Where a VASP relies on another VASP for business introduction or in the conduct of CDD, the VASP-to-VASP reliance for CDD, particularly in the context of VA transfers, should occur in a manner consistent and compliant with the requirements of Recommendation 16.
 122. **Recommendation 18** requires countries to require obliged entities, such as VASPs, to have internal controls in place with a view to establishing the effectiveness of the AML/CFT policies and processes and the quality of the risk management across its operations, departments, branches and subsidiaries, both domestically and, where relevant, abroad. Those internal controls should include appropriate governance arrangements where responsibility for AML/CFT is clearly allocated and a compliance officer is appointed at management level; controls to monitor the integrity of staff, which are implemented in accordance with the applicable local legislation; ongoing training of staff; and an (external or internal) independent audit function to test the system.
 123. **Recommendation 19** requires countries to require obliged entities, such as VASPs, to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons from higher risk countries, which include countries for which enhanced due diligence measures are called for by the FATF. This is of specific relevance for VA activities and VASPs, given the cross-border nature of their activities.
 124. **Recommendation 20** requires all FIs that suspect or have reasonable grounds to suspect that funds are the proceeds of crime or are related to terrorist financing to report their suspicions promptly to the relevant FIU. Accordingly, countries should ensure that VASPs as well as any other obliged entities that engage in covered VA activities file STRs (see Section IV for additional information specific to VASPs and other obliged entities).
 125. Consistent with paragraph 7 of INR. 15 relating to the application of the preventive measures and as discussed above in the context of Recommendation 16, countries also should require VASPs to comply with all of the relevant requirements of Recommendation 16 in the countries in which they operate (again, see Section IV for additional information).
 126. In some jurisdictions that already implement comprehensive AML/CFT obligations for VASPs and other obliged entities that engage in VA activities, STRs that reference VAs have proven invaluable in furthering law enforcement investigative efforts as well as for improving the FIU's ability to better understand and analyse both providers and activities in the VA

ecosystem.²⁰ Countries should consider whether updates to their existing reporting mechanisms or forms are necessary in order to enable providers or other obliged entities to report specific indicators that may be associated with VA activity, such as device identifiers, IP addresses with associated time stamps, VA wallet addresses, and transaction hashes.

127. **Recommendation 21** relates to the tipping-off and confidentiality measures applicable to FIs under the FATF Recommendations. Countries should also apply such measures to VASPs, as set forth in paragraph 7 of INR. 15 relating to the application of the preventive measures. VASPs, their directors, officers, and employees, where applicable, should be protected by law from criminal and civil liability for breach of any restriction on disclosure of information and prohibited by law from disclosing (or “tipping-off”) STRs, as detailed in Recommendation 21.

Transparency and Beneficial Ownership of Legal Persons and Arrangements

128. **Recommendations 24 and 25.** The FATF Glossary defines VASPs as *any natural or legal person that conducts as a business the activities or operations specified in the VASP definition*. Recommendations 24 and 25 explicitly note that countries should take measures to prevent the misuse of legal persons and arrangements for money laundering and terrorist financing. As with FIs and DNFBPs, countries should therefore take measures to prevent the misuse of VASPs and consider measures to facilitate access to beneficial ownership and control information by VASPs undertaking the requirements set out in Recommendations 10 and 22.

Operational and Law Enforcement

129. **Recommendation 29.** STRs filed by VASPs (or other obliged entities such as traditional FIs that may be operating in the VA space or engaging in covered VA activities) under Recommendation 20 must be filed with the FIU. Additionally, FIUs should be able to obtain additional information from reporting entities in their jurisdiction, which include VASPs, and should have access on a timely basis to the financial, administrative, and law enforcement information that the FIU requires to undertake its functions properly.
130. Readers of this Guidance should note that **Recommendation 30** is addressed above in the funds- or value-based terms section of the Recommendation-by-Recommendation analysis.
131. **Recommendation 31.** As with FIs and DNFBPs, countries and competent authorities should be able to obtain access to all necessary documents and information, including powers to use compulsory measures for the production of records, held by VASPs. They should have effective mechanisms in place to identify whether natural or legal persons such as VASPs hold or control VA accounts or wallets and mechanisms for ensuring that competent authorities have a process to identify assets, including VAs, without prior notification to the owner. The application of Recommendation 31 is particularly important for countries and their competent authorities in addressing and mitigating the ML/TF risks associated with covered VA activities and VASPs.
132. **Recommendation 32.** Jurisdictions should take a risk-based approach in considering whether to apply Recommendation 32 to covered VA activities and VASPs. Specifically, jurisdictions should consider in their risk-based approach (a) whether the activities of VASPs and with VAs fall under the parameters of transportation of physical monetary instruments and (b) how

²⁰ For example, STRs filed both by depository institutions and VASPs (specifically, exchangers) enabled U.S. law enforcement to take action in 2017 against BTC-e—an Internet-based money transmitter that exchanged fiat currency as well as VAs and facilitated transactions involving ransomware, computer hacking, identity theft, tax fraud schemes, public corruption, and drug trafficking—by helping them to identify VA wallet addresses used by BTC-e and detect different illicit streams of activity moving through the exchange.

establishing requirements for declaration and systems for detection of cross-border movement of such assets would work in practice as well as how they would mitigate ML/TF risks in their jurisdiction.

133. As with Recommendation 30, readers of this Guidance should note that **Recommendation 33** is addressed above in the funds- or value-based terms section.
134. **Recommendation 34** is a vital component in countries' approaches to identifying and addressing the ML/TF risks associated with VA activities and VASPs, as well as in relation to the VAs themselves. The relevant competent authorities should establish guidelines and provide feedback that will assist VASPs (as well as other obliged entities, including traditional FIs) in applying national measures to combat money laundering and terrorist financing and, in particular, in detecting and reporting suspicious transactions—whether virtual/fiat or virtual/virtual.

International Co-operation

135. **Recommendations 36 through 40.** Given the cross-border and mobile nature of VA activities and the VASP sector, international co-operation and the implementation of Recommendations 36 through 40 by countries and competent authorities is critical, particularly the measures applicable to countries and competent authorities in Recommendations 37 through 40. Moreover, effective implementation of the requirements relating to international co-operation is important for limiting the ability of providers' of VA activities in one jurisdiction from having an unfair competitive advantage over providers in other, potentially more regulated, jurisdictions and limit jurisdiction shopping or hopping or regulatory arbitrage.
136. Recognizing that effective regulation, supervision, and enforcement relating to the VASP sector requires a global approach and a level regulatory framework across jurisdictions, paragraph 8 of INR. 15 underscores the importance of the application of Recommendations 37 through 40 for mitigating the risks associated with VAs, covered VA activities, and VASPs. Countries should have in place the tools necessary to co-operate with one another, provide mutual legal assistance (Recommendation 37); help identify, freeze, seize, and confiscate the proceeds and instrumentalities of crime that may take the form of VAs as well as other traditional assets associated with VASP activities (Recommendation 38); and provide effective extradition assistance in the context of VA-related crimes or illicit actors who engage in illicit activities (Recommendation 39), among other international capabilities.
137. As with other Recommendations that include funds- or value-based terms, countries should apply the confiscation and provisional measures relating to "property laundered from, proceeds from, instrumentalities used in, or instrumentalities intended for use in money laundering, predicate offences, or terrorist financing; or property of corresponding value" in the context of VAs.
138. Paragraph 8 of INR. 15 also specifically requests that supervisors of VASPs exchange information promptly and constructively with their foreign counterparts, regardless of the supervisors' nature or status or differences in the nomenclature or status of VASPs (see sub-sections 3.1.4 and 3.18 above).
139. International co-operation is also relevant in the context of VASPs that seek to register or license themselves in one jurisdiction but provide products or services "offshore" to customers located in other jurisdictions. It is important that FIUs co-operate and exchange information on relevant STRs with their counterparts in a timely manner, especially in relation to cross-border VA activities or VASP operations. Sufficient oversight and regulatory control of VASPs operating in their jurisdiction enables countries to better provide investigatory assistance and other international co-operation in the VA space. At present, the lack of regulation and investigation capacity in most countries may present obstacles to countries' ability to provide

meaningful international co-operation. Moreover, many countries do not have legal frameworks that allow them to criminalize certain VA-related ML/TF activities, which could further limit their ability to provide effective mutual legal assistance in situations where dual criminality is required.

DNFBPs that Engage in or Provide Covered VA Activities

140. When a DNFBP engages in VASP activity (*e.g.*, when a casino offers VA-based gaming or engages in other covered VA activities, products, or services), countries should subject the entity to all of the measures for VASPs set forth in the FATF Recommendations. Countries should note, for example, that Recommendations 22 and 23 set out the CDD, recordkeeping, and other requirements for certain types of DNFBPs in the following situations: (a) casinos, (b) real estate agents, (c) dealers in precious metals and stones, (d) lawyers, notaries, other independent legal professionals and accountants, and (e) trust and company service providers. Recommendation 22 specifically notes that the requirements set out in Recommendations 10, 11, 12, 15, and 17 apply to DNFBPs. Thus, in considering how to regulate and supervise and apply the preventive measures to DNFBPs that engage in VASP activities, countries should refer to the application of Recommendations 10, 11, 12, 15, and 17, among other Recommendations relevant to VASPs, and apply the appropriate CDD, recordkeeping, and other measures accordingly.
141. Similarly, Recommendation 28 requires countries and competent authorities to subject DNFBPs to regulatory and supervisory measures, as set out in the FATF Recommendations. As stated previously, countries should subject VASPs, including DNFBPs that engage in VASP activities, to a level of supervision and regulation on par with FIs and not to DNFBP-level supervision. Where a DNFBP engages in covered VASP activities (*e.g.*, a casino that provides VA products and services or engages in covered VA activities), countries should subject the DNFBP to a higher level of supervision (*e.g.*, “DNFBP plus” supervision), consistent with the higher level of supervision for all VASPs, which is equivalent to the level of supervision and regulation for FIs as laid out in Recommendations 26 and 27. In such instances, the entity is, in essence, a VASP engaging in specified financial activities and not a DNFBP, regardless of what a country may term, call, or label such an entity, institution, or product or service provider. This approach by countries will help to ensure a level regulatory playing field across the VASP sector globally and a level of supervision for VASPs that is consistent with and appropriate for the types of activities in which they engage.

Risk-Based Approach to Supervision or Monitoring of VASPs

Understanding the ML/TF Risks

142. The risk-based approach to AML/CFT aims to develop prevention or mitigation measures that are commensurate with the ML/TF risks that countries and the relevant obliged entities identify. In the case of supervision, the risk-based approach applies to the way in which supervisory authorities allocate their resources. It also applies to supervisors discharging their functions in a way that is conducive to the application of the risk-based approach by VASPs.
143. An effective risk-based regime should reflect a country’s policy, legal, and regulatory approach. The national policy, legal, and regulatory framework should also reflect the broader context of financial sector policy objectives that the country is pursuing, including financial inclusion, financial stability, financial integrity, and financial consumer protection goals, and consider such factors as market competition. The extent to which the national framework allows VASPs to apply a risk-based approach should also reflect the nature, diversity, and maturity of the VASP sector and its risk profile as well as the ML/TF associated with individual VASPs and specific VA products, services, or activities.

144. Supervisors should also develop a deep understanding of the VASP market, its structure, and its role in the financial system and the country's economy to better inform their assessment of risk in the sector. This may require investing in training, personnel, or other resources that enable supervisors to gain the practical skillsets and expertise needed to regulate and supervise the range of VA providers and activities described in the VA services or business models at the onset of this Guidance.
145. Supervisors should draw on a variety of sources to identify and assess the ML/TF risks associated with VA products, services, and activities as well as with VASPs. Such sources should include, but are not limited to, the jurisdiction's national or sectoral risk assessments, domestic or international typologies and supervisory expertise, and FIU guidance and feedback. Where competent authorities do not adequately understand the VASP sector or broader VA ecosystem in the country, it may be appropriate for competent authorities to undertake a more targeted sectoral risk assessment in relation to the VASP sector and/or VA environment in order to develop a national-level understanding of the relevant ML/TF risks and to inform the institutional assessments that should be undertaken by VASPs.
146. Access to information about ML/TF risks is fundamental for an effective risk-based approach. Recommendation 1 (see INR. 1.3) requires countries, including supervisors, to take appropriate steps to identify and assess ML/TF risks for the country on an ongoing basis in order to make information available for AML/CFT risk assessments conducted by FIs and DNFBPs, including VASPs. Countries, including supervisors, should keep the risk assessments up-to-date and should have mechanisms to provide appropriate information on the results to all relevant competent authorities, FIs, and DNFBPs, including VASPs. In situations where some parts of the VASP sector have potentially limited capacity to identify the ML/TF risks associated with VA products, services, or activities, countries, including supervisors, should work with the sector to understand its risks and to help the private sector in developing its own understanding of the risks. Depending on the capacity of the VASP sector, general information or more granular information and support may be required.
147. In considering individual VASPs or particular VA products, services, or activities, supervisors should take into account the level of risk associated with the VASPs' products and services, business models, corporate governance arrangements, financial and accounting information, delivery channels, customer profiles, geographic location, countries of operation, VASPs' level of compliance with AML/CFT measures, as well as the risks associated with specific VA tokens or products that potentially obfuscate transactions or undermine the ability of VASPs and supervisors to implement effective AML/CFT measures. Supervisors should also look at the controls in place in a VASP, including the quality of a VASP's risk management policy or the functioning of its internal oversight mechanisms. Other information that may be relevant in the AML/CFT context includes the fitness and propriety of the VASP's management and compliance functions.
148. Some of the aforementioned information can be obtained through prudential supervisors in countries where VASPs or other obliged entities that engage in covered VA activities are subject to prudential regulations (*i.e.*, where VASPs are traditional FIs subject to the Core Principles,²¹ such as banks, insurance companies, securities providers, or investment companies), which therefore involves appropriate information sharing and collaboration between prudential and AML/CFT supervisors, especially when the responsibilities belong to separate agencies. In other regulatory models, such as those that focus on licensing or

²¹ Under the FATF Recommendations, "core principles" refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulated issued by the International Organization of Securities Commissions, and the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.

- registration of VASPs at the national level but have shared oversight and enforcement at the state level, information sharing should include the sharing of examination findings.
149. Where relevant, information from other stakeholders, such as supervisors (including overseas supervisors and supervisors of payment systems and instruments as well as securities, commodities and derivatives thereof), the FIU and law enforcement agencies may also be helpful for supervisors in determining the extent to which a VASP effectively manages the ML/TF risks to which it is exposed. Some regimes, such as those that only require registration (without extensive background testing) may still enable law enforcement and regulators to be aware of the existence of a VASP, its lines of business, its particular VA products or services, and/or its controlling interests.
 150. Supervisors should review their assessment of the risk profiles of both the VASP sector and VASPs periodically and when VASPs' circumstances change materially or relevant new threats emerge. Examples of existing country supervisory practices for VASPs or the broader VASP sector as well as country examples relating to ML/TF risks associated with particular VA products, services, or business models can be found in Section V of this Guidance.

Mitigating the ML/TF Risks

151. The FATF Recommendations require supervisors to allocate and prioritize more supervisory resources to areas of higher ML/TF risk. This means that supervisors should determine the frequency and intensity of periodic assessments based on the level of ML/TF risks to which the sector and individual VASPs are exposed. Supervisors should give priority to the potential areas of higher risk, either within the individual VASP (*e.g.*, to the particular products, services, or business lines that a VASP may offer, such as particular VAs or VA services like AECs or mixers and tumblers that may further obfuscate transactions or undermine the VASP's ability to implement CDD measures) or to VASPs operating in a particular sector (*e.g.*, to VASPs that only or predominantly facilitate virtual-to-virtual financial activities or that offer particular VA obfuscating products or services, or VASPs that facilitate VA transfers on behalf of their customers to individual users that are not customers of another regulated entity, such as a beneficiary institution). If a jurisdiction chooses to classify an entire sector as higher risk, countries should still understand and be able to provide some explanation and granularity on the categorisation of individual VASPs within the sector based on their customer base, the countries they deal with, and their applicable AML/CFT controls.
152. It is also important that competent authorities acknowledge that in a risk-based regime, not all VASPs will adopt identical AML/CFT controls and that single, unwitting and isolated incidents involving the transfer or exchange of illicit proceeds do not necessarily invalidate the integrity of a VASP's AML/CFT controls. On the other hand, VASPs should understand that a flexible risk-based approach does not exempt them from applying effective AML/CFT controls.
153. Examples of ways in which supervisors can adjust their approach include:
 - a) *Adjusting the type of AML/CFT supervision or monitoring*: supervisors should employ both offsite and onsite access to all relevant risk and compliance information. However, to the extent permitted by their regime, supervisors can determine the correct mix of offsite and onsite supervision or monitoring of VASPs. Offsite supervision alone may not be appropriate in higher risk situations. However, where supervisory findings in previous examinations (either offsite or onsite) suggest a low risk for ML/TF, resources can be allocated to focus on higher risk VASPs. In that case, lower risk VASPs could be supervised offsite, for example through transaction analysis and questionnaires.

- b) *Adjusting the frequency and nature of ongoing AML/CFT supervision or monitoring:* supervisors should adjust the frequency of AML/CFT examinations in line with the risks identified and combine periodic reviews and ad hoc AML/CFT supervision as issues emerge (e.g., as a result of whistleblowing, information from law enforcement, analysis of financial reporting or other supervisory findings). Other risk-based approaches to supervision could include consideration of the geographic location, registration or licensing status, customer base, transaction type (e.g., virtual/fiat or virtual/virtual transactions), VA type, number of accounts or wallets, revenue, products or services offered (e.g., more transparent services versus those products or services that obfuscate transactions, such as AECs), prior history of non-compliance, and/or significant changes in management.
 - c) *Adjusting the intensity of AML/CFT supervision or monitoring:* supervisors should decide on the appropriate scope or level of assessment in line with the risks identified, with the aim of assessing the adequacy of VASPs' policies and procedures that are designed to prevent VASPs' abuse. Examples of more intensive supervision could include detailed testing of systems and files to verify the implementation and adequacy of the VASPs' risk assessment, reporting and recordkeeping policies and processes, internal auditing, interviews with operation staff, senior management and the Board of Directors, where applicable.
154. Supervisors should use their findings to review and update their ML/TF risk assessments and, where necessary, consider whether their approach to AML/CFT supervision and AML/CFT rules and guidance remains adequate. Whenever appropriate, and in compliance with any relevant standards or requirements relating to the confidentiality of such information, supervisors should communicate their findings to VASPs to enable them to enhance the quality of their risk-based approaches.

General Approach

155. Supervisors should understand the ML/TF risks faced by VASPs or associated with the VASP sector. Supervisors should have a comprehensive understanding of higher and lower risk lines of business or particular VA products, services or activities, with a particularly thorough understanding of the higher-risk products, services or activities.
156. Supervisors should ensure that their staff is equipped to assess whether a VASP's policies, procedures, and controls are appropriate and proportional in view of the VASP's risk assessment and risk management procedures. To support supervisors' understanding of the overall strength of measures in the VASP sector, countries could consider conducting a comparative analysis of VASPs' AML/CFT programs in order to further inform their judgment of the quality of an individual VASP's controls.
157. In the context of the risk-based approach, supervisors should determine whether a VASP's AML/CFT compliance and risk management program is adequate to (i) meet the regulatory requirements, and (ii) appropriately and effectively mitigate and manage the relevant risks. In doing so, supervisors should take into account the VASP's own risk assessment. In the case of VASPs that operate across different jurisdictions on the basis of multiple licenses or registrations, given the cross-border nature of covered VA activities, the supervisor that licenses or registers the natural or legal person VASP should take into consideration the risks to which the VASP is exposed and the extent to which those risks are adequately mitigated.
158. As part of their examination procedures, supervisors should communicate their findings and views about an individual VASP's AML/CFT controls and communicate clearly their

expectations of the measures needed for VASPs to comply with the applicable legal and regulatory frameworks. In jurisdictions where VA financial activities may implicate multiple competent authorities, supervisory counterparts within the jurisdiction should also co-ordinate with one another, where applicable, to effectively and clearly communicate their expectations to VASPs as well as to other obliged entities that may engage in VA activities or provide VA products or services. This is particularly important in the context of VASPs that engage in various types of regulated VA activity (*e.g.*, VA money or value transfer services or securities, commodities or derivatives activity) or in VA financial activities that may implicate various banking, securities, commodities, or other regulators.

Guidance

159. Supervisors should communicate their expectations of VASPs' compliance with their legal and regulatory obligations and may consider engaging in a consultative process, where appropriate, with relevant stakeholders. Such guidance may be in the form of high-level requirements based on desired outcomes, risk-based obligations, and information about how supervisors interpret relevant legislation or regulation or more detailed guidance about how VASPs might best apply particular AML/CFT controls.
160. Supervisors and other competent authorities may consider the guidance and input of VA technical experts in order to develop a deeper understanding of the relevant business models and operations of VASPs, their potential exposure to ML/TF risks, as well as the ML/TF risks associated with particular VA types or specific covered VA activities and to make an informed judgment about the mitigation measures in place or needed.
161. As discussed previously, providing guidance for and feedback to the VASP sector is essential and is a requirement under Recommendation 34. The guidance could include best practices that enable VASPs to undertake assessments and develop risk mitigation and compliance management systems to meet their legal and regulatory obligations. Supporting ongoing and effective communication between supervisors and VASPs is an essential component of the successful implementation of a risk-based approach.
162. Supervisors of VASPs should also consider liaising with other relevant domestic regulatory and supervisory authorities to secure a coherent interpretation of VASPs' legal obligations and to promote a level playing field, including between VASPs and between VASPs and other obliged entities such as FIs and DNFBCs. Such co-ordination is particularly important where more than one supervisor is responsible for supervision (*e.g.*, where the prudential supervisor and the AML/CFT supervisors are in different agencies or in separate divisions of the same agency). It also is particularly relevant in the context of VASPs that provide various products or services or engage in different financial activities that may fall under the purview of different regulatory or supervisory authorities within a particular jurisdiction. Multiple sources of guidance should not create opportunities for regulatory arbitrage, loopholes, or unnecessary confusion among VASPs. When possible, relevant regulatory and supervisory authorities in a jurisdiction should consider preparing joint guidance.

Training

163. Training is important for supervision staff to understand the VASP sector and the various business models that exist. In particular, supervisors should ensure that staff are trained to assess the quality of a VASP's ML/TF risk assessment and to consider the adequacy, proportionality, effectiveness, and efficiency of the VASP's AML/CFT policies, procedures, and internal controls in light of its risk assessment.
164. Training should allow supervisory staff to form sound judgements about the quality of the VASP's risk assessments and the adequacy and proportionality of a VASP's AML/CFT controls.

It should also aim at achieving consistency in the supervisory approach at a national level in cases where there are multiple competent supervisory authorities or when the national supervisory model is devolved or fragmented.

165. Similarly, countries should consider opportunities for public-private sector training and collaboration to further educate and raise awareness among both operational and other competent authorities and industry on various issues relating to VAs and VASP activities.

Information Exchange

166. Information exchange between the public and private sector is important and should form an integral part of a country's strategy for combating ML/TF in the context of VA and VASP activities. Public authorities should share risk information, where possible, to better help inform the risk assessments of VASPs. The type of information relating to risks in the VA space that the public and private sectors could share include:
- a) ML/TF risk assessments;
 - b) Typologies and methodologies of how money launderers or terrorist financiers misuse VASPs, a particular VA mechanism over another (*e.g.*, VA transfer or exchange activities versus VA issuance activities in the context of money laundering or terrorist financing) or VAs more generally;
 - c) General feedback on the quality and usefulness of STRs and other relevant reports;
 - d) Information on suspicious indicators associated with VA activities or VASP transactions;
 - e) Targeted unclassified intelligence, where appropriate and subject to the relevant safeguards such as confidentiality agreements; and
 - f) Countries, persons, or organisations whose assets or transactions should be frozen pursuant to targeted financial sanctions as required by Recommendation 6.
167. Further, countries should consider how they might share information with the private sector in order to help the private sector, including VASPs, better understand the nature of law enforcement information requests or other government requests for information or to help shape the nature of the requests so that VASPs can provide more accurate and specific information, where applicable, to competent authorities.
168. Domestic co-operation and information exchange between the supervisors of the banking, securities, commodities, and derivatives sectors and the VASP sector; among law enforcement, intelligence, FIU and VASP supervisors; and between the FIU and the supervisor(s) of the VASP sector are also of vital importance for effective monitoring and supervision of VASPs.
169. Similarly, in line with Recommendation 40, cross-border information sharing by authorities and the private sector with their international counterparts is critical in the VASP sector, taking into account the cross-border nature and multi-jurisdictional reach of VASPs.

SECTION IV – APPLICATION OF FATF STANDARDS TO VASPS AND OTHER OBLIGED ENTITIES THAT ENGAGE IN OR PROVIDE COVERED VA ACTIVITIES

170. The FATF Recommendations apply both to countries as well as to VASPs and other obliged entities that provide covered VA-related services or financial activities or operations (“other obliged entities”), including banks, securities broker-dealers, and other FIs. Accordingly, Section IV provides additional guidance specific to VASPs and other obliged entities that may engage in covered VA activities.
171. In addition to identifying, assessing, and taking effective action to mitigate their ML/TF risks, as described under **Recommendation 1**, VASPs and other obliged entities in particular should apply all of the preventive measures in Recommendations 9 through 21 as set forth above in Section III, including in the context of CDD, when engaging in any covered VA activities. Similarly, DNFBPs should be aware of their AML/CFT obligations when engaging in covered VA activities as set forth in INR. 15 and as described in sub-section 3.1.9.
172. Readers of this Guidance should note that the below paragraphs relating to individual preventive measures and FATF Recommendations are intended to provide additional specific guidance for VASPs and other obliged entities on certain issues. The lack of a dedicated paragraph for each FATF Recommendation within the preventive measures, as provided in Section III, for example, does not mean that the respective Recommendations or preventive measures contained therein do not also apply to VASPs and other obliged entities that engage in or provide VA activities.
173. **Recommendation 10** sets forth the required CDD measures that FIs must implement for all customers, including identifying the customer and verifying the customer’s identity using reliable, independent source documents, data or information; identifying the beneficial owner; understanding and obtaining information on the purpose and intended nature of the business relationship; and conducting ongoing due diligence on the relationship and scrutiny of transactions.
174. Recommendation 10 also describes the scenarios under which FIs must undertake CDD measures, including in the context of establishing business relations, carrying out occasional transactions above the designated threshold (USD/EUR 1 000 for VA transactions), carrying out occasional transactions that are wire transfers as set forth under Recommendation 16 and its Interpretive Note (also USD/EUR 1 000 for VA transfers), where there is a suspicion of ML/TF, or when the FI doubts the veracity or adequacy of previously obtained customer identification data. While countries may adopt a *de minimis* threshold of USD/EUR 1 000 under their national framework for VA transactions that they deem are occasional (as described in Section III) or for VA transfers, all of which are treated as cross-border qualifying wire transfers for the purposes of applying Recommendation 16, it should be underscored that banks, broker-dealers, and other FIs must still adhere to their respective CDD thresholds when engaging in covered VA activities. For DNFBPs, such as casinos, that engage in covered VA activity, they should apply the *de minimis* threshold of USD/EUR 1 000 for occasional transactions and for occasional transactions that are wire transfers as described in Section III and as discussed below. As noted in Section III in the context of countries, VASPs, in establishing their operating procedures and processes when accepting customers and facilitating transactions, should consider how they can determine and ensure that transactions are in fact only conducted on a one-off or occasional basis rather than on a more consistent (*i.e.*, non-occasional) basis.
175. Although the designated thresholds above which casinos and dealers in precious metals and stones must conduct CDD for occasional transactions and for occasional transactions that are wire transfers are USD/EUR 3 000 and USD/EUR 15 000 respectively, when DNFBPs engage in any covered VA or VASP activities, they are subject to the CDD standards as set forth under

INR. 15 (*i.e.*, a *de minimis* threshold of USD/EUR 1 000 for occasional transactions and for occasional transactions that are wire transfers).

176. Regardless of the nature of the relationship or VA transaction, VASPs and other obliged entities should have in place CDD procedures that they effectively implement and use to identify and verify on a risk basis the identity of a customer, including when establishing business relations with that customer; where they have suspicions of ML/TF, regardless of any exemption of thresholds; and where they have doubts about the veracity or adequacy of previously obtained identification data.
177. Like other obliged entities, in conducting CDD to fulfil their obligations under Recommendation 10, VASPs should obtain and verify the customer identification/verification information required under national law. Typically, required customer identification information includes information on the customer's name and further identifiers such as physical address, date of birth, and a unique national identifier number (*e.g.*, national identity number or passport number). Depending upon the requirements of their national legal frameworks, VASPs are also encouraged to collect additional information to assist them in verifying the customer's identity when establishing the business relationship (*i.e.*, at onboarding); authenticate the identity of customers for account access; help determine the customer's business and risk profile and conduct ongoing due diligence on the business relationship; and mitigate the ML/TF risks associated with the customer and the customer's financial activities. Such additional, non-core identity information, which some VASPs currently collect, could include, for example an IP address with an associated time stamp; geo-location data; device identifiers; VA wallet addresses; and transaction hashes.
178. For covered VA activities, the verification of customer and beneficial ownership information by VASPs should be completed before or during the course of establishing the relationship.²²
179. Based on a holistic view of the information obtained in the context of their application of CDD measures—which could include both traditional information and non-traditional information as describe above—VASPs and other obliged entities should be able to prepare a customer risk profile in appropriate cases. A customer's profile will determine the level and type of ongoing monitoring potentially necessary and support the VASPs' decision whether to enter into, continue, or terminate the business relationship. Risk profiles can apply at the customer level (*e.g.*, nature and volume of trading activity, origin of virtual funds deposited, etc.) or at the cluster level, where a cluster of customers displays homogenous characteristics (*e.g.*, clients conducting similar types of VA transactions or involving the same VA). VASPs should periodically update customer risk profiles of business relationships in order to apply the appropriate level of CDD.
180. If a VASP uncovers VA addresses that it has decided not to establish or continue business relations with or transact with due to suspicions of ML/TF, the VASP should consider making available its list of "blacklisted wallet addresses," subject to the laws of the VASP's jurisdiction. A VASP should screen its customer's and counterparty's wallet addresses against such available blacklisted wallet addresses as part of its ongoing monitoring. A VASP should make its own risk-based assessment and determined whether additional mitigating or preventive actions are warranted if there is a positive hit.
181. VASPs and other obliged entities that engage in covered VA activities may adjust the extent of CDD measures, to the extent permitted or required by their national regulatory requirements, in line with the ML/TF risks associated with the individual business relationships, products or services, and VA activities, as discussed above under the application of Recommendation 1. VASPs and other obliged entities must therefore increase the amount or type of information obtained or the extent to which they verify such information where the risks associated with

²² See also 2015 VC Guidance, paragraph 45.

the business relationship or VA activities is higher, as described in Section III. Similarly, VASPs and other obliged entities may also simplify the extent of the CDD measures where the risk associated with the business relationship of activities is lower. However, VASPs and other obliged entities may not apply simplified CDD or an exemption from the other preventive measures simply on the basis that natural or legal persons carry out the VA activities or services on an occasional or very limited basis (INR. 1.6(b)). Further, simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing or where specific higher-risk scenarios apply (see Section III for an explanation of potentially higher-risk situations)

182. Ongoing monitoring on a risk basis means scrutinizing transactions to determine whether those transactions are consistent with the VASP's (or other obliged entity's) information about the customer and the nature and purpose of the business relationship, wherever appropriate. Monitoring transactions also involves identifying changes to the customer profile (*e.g.*, the customer's behaviour, use of products, and the amounts involved) and keeping it up-to-date, which may require the application of enhanced CDD measures. Monitoring transactions is an essential component in identifying transactions that are potentially suspicious, including in the context of VA transactions. Transactions that do not fit the behaviour expected from a customer profile, or that deviate from the usual pattern of transactions, may be potentially suspicious.
183. Monitoring should be carried out on a continuous basis and may also be triggered by specific transactions. Where large volumes of transactions occur on a regular basis, automated systems may be the only realistic method of monitoring transactions, and flagged transactions should go through human/expert analysis to determine if such transactions are suspicious. VASPs and other obliged entities should understand their operating rules, verify their integrity on a regular basis, and check that they account for the identified ML/TF risks associated with VAs, products or services or VA financial activities.
184. VASPs and other obliged entities should adjust the extent and depth of their monitoring in line with their institutional risk assessment and individual customer risk profiles. Enhanced monitoring should be required for higher-risk situations (as described in Sections II and III) and extend beyond the immediate transaction between the VASP or its customer or counterparty. The adequacy of monitoring systems and the factors that lead VASPs and other obliged entities to adjust the level of monitoring should be reviewed regularly for continued relevance to their AML/CFT risk programme.
185. Monitoring under a risk-based approach allows VASPs or other obliged entities to create monetary or other thresholds to determine which activities will be reviewed. Defined situations or thresholds used for this purpose should be reviewed on a regular basis to determine their adequacy for the risk levels established. VASP and other obliged entities should document and state clearly the criteria and parameters used for customer segmentation and for the allocation of a risk level for each of the clusters of customers, where applicable. The criteria applied to decide the frequency and intensity of the monitoring of different customer (or even VA product) segments should also be transparent. To this end, VASPs and other obliged entities should properly document, retain, and communicate to the relevant personnel and national competent authorities the results of their monitoring as well as any queries raised and resolved.

186. **Recommendation 12.** For domestic PEPs²³ and international organisation PEPs,²⁴ obliged entities, such as VASPs, must take reasonable measures to determine whether a customer or beneficial owner is a domestic or international organisation PEP and then assess the risk of the business relationship. For higher-risk business relationships with domestic PEPs and international organisation PEPs, VASPs and other obliged entities should take additional measures consistent with those applicable to foreign PEPs, including identifying the source of wealth and source of funds when relevant.²⁵
187. **Recommendation 16.** As noted in Section III, providers in this space must comply with the requirements of Recommendation 16, including the obligation to obtain, hold, and transmit required originator and beneficiary information associated with VA transfers in order to identify and report suspicious transactions, take freezing actions, and prohibit transactions with designated persons and entities. The requirements apply to both VASPs and other obliged entities such as FIs when they send or receive VA transfers on behalf of a customer.
188. The FATF is technology-neutral and does not prescribe a particular technology or software approach that providers should deploy to comply with Recommendation 16. As noted previously, any technology or software solution is acceptable, so long as it enables the ordering and beneficiary institution (where present in the transaction) to comply with its AML/CFT obligations. For example, a solution for obtaining, holding, and transmitting the required information (in addition to complying with the various other requirements of Recommendation 16) could be code that is built into the VA transfer's underlying DLT transaction protocol or that runs on top of the DLT platform (*e.g.*, using a smart contract, multiple-signature, or any other technology); an independent (*i.e.*, non-DLT) messaging platform or application program interface (API); or any other effective means for complying with the Recommendation 16 measures.
189. VASPs and other obliged entities in VA transfers, whether as an ordering or beneficiary institution, should consider how they might leverage existing commercially available technology to comply with the requirements of Recommendation 16, and specifically the requirements of INR. 15, paragraph 7(b). Examples of existing technologies that providers could consider as a foundation for enabling the identification of beneficiaries of VA transfers as well as the transmission of required originator and beneficiary in near real-time before a VA transfer is conducted on a DLT platform include:
- a) *Public and private keys*, which are created in pairs for each entity involved in a transmission and encrypt and decrypt information during the initial part of the transmission so that only the sender and recipient of the transmission can decrypt and read the information, wherein the public key is available to everyone while the private key is known only to the creator of the keys;
 - b) *Transport Layer Security/Secure Sockets Layer (TLS/SSL) connections*, which make use of public and private keys among parties when establishing a connection and secure almost all transmissions on the Internet, including

²³ “Domestic PEPs” are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials (FATF Glossary).

²⁴ “Persons who are or have been entrusted with a prominent function by an international organisation” refers to members of senior management, *i.e.*, directors, deputy directors, and members of the board or equivalent functions (FATF Glossary).

²⁵ Further information on PEPs is set out in the 2013 FATF [Guidance on Politically Exposed Persons \(Recommendations 12 and 22\)](#).

- emails, web browsing, logins, and financial transactions, ensuring that all data that passes between a web server and a browser remains private and secure;
- c) *X.509 certificates*, which are digital certificates administered by certificate authorities that use the X.509 PKI standard to verify that a public key belongs to the user, computer, or service identity in the certificate and which are used worldwide across public and private sectors;
 - d) *X.509 attribute certificates*, which can encode attributes (such as name, date of birth, address, and unique identifier number), are attached cryptographically to the X.509 certificate, and are administered by attribute certificate authorities;
 - e) *API technology*, which provides routines, protocols, and tools for building software applications and specifies how software components should interact; as well as
 - f) Other commercially available technology or potential software or data sharing solutions.
190. As set forth in INR. 15, paragraph 7(b), it is vital that VASPs and other obliged entities that engage in VA transfers submit the required information in a secure manner, so as to protect the customer information associated with the VA transfers against unauthorized disclosures and enable receiving entities to effectively comply with their own AML/CFT obligations, including identifying suspicious VA transfers, taking freezing actions, and prohibiting transactions with designated persons and entities. Further, and as highlighted in Section III, it is essential that providers submit the required information immediately—that is, simultaneously or concurrent with the transfer itself—particularly given the cross-border nature, global reach, and transaction speed of VA activities.
191. **Recommendation 18.** The successful implementation and effective operation of a risk-based approach to AML/CFT depends on strong senior management leadership, which includes oversight of the development and implementation of the risk-based approach across the VASP sector. Recommendation 18 also requires information sharing within the group, where relevant, regarding in particular unusual transactions or activities.
192. VASP and other obliged entities should maintain AML/CFT programmes and systems that are adequate to manage and mitigate their risks. The nature and extent of the AML/CFT controls will depend upon a number of factors, including the nature, scale and complexity of the VASP’s business, the diversity of its operations, including geographical diversity, its customer base, product and activity profile, and the degree of risk associated with each area of its operations, among other factors.
193. **Recommendation 20.** VASPs and other obliged entities that engage in or provide VA activities, products, and services should have the ability to flag for further analysis any unusual or suspicious movements of funds or transactions—including those involving or relating to VAs—or activity that is otherwise indicative of potential involvement in illicit activity regardless of whether the transactions or activities are fiat-to-fiat, virtual-to-virtual, fiat-to-virtual, or virtual-to-fiat in nature. VASPs and other obliged entities should have appropriate systems so that such funds or transactions are scrutinised in a timely manner and a determination can be made as to whether funds or transactions are suspicious.
194. VASPs and other obliged entities should promptly report funds or transactions, including those involving or relating to VAs and/or providers that are suspicious to the FIU and in the manner specified by competent authorities. The processes that VASPs and other obliged entities put in place to escalate their suspicions and ultimately report to the FIU should reflect this. While

VASPs and other obliged entities can apply the policies and processes that lead them to form a suspicion on a risk-sensitive basis, they should report their ML/TF suspicions once formed and regardless of the amount of the transaction or whether the transaction has completed. The obligation for VASPs and other obliged entities to report suspicious transactions is therefore not risk-based, nor does the act of reporting discharge them from their other AML/CFT obligations. Further, VASPs and other obliged entities should comply with applicable STR requirements even when operating across different jurisdictions.

195. Consistent with INR. 15 and in relation to Recommendation 16, in the case of a VASP (or other obliged entity) that controls both the ordering and the beneficiary side of a VA funds or wire transfer, the VASP or other obliged entity should take into account all of the information from both the ordering and beneficiary sides in order to determine whether the information gives rise to suspicion and, where necessary, file an STR with the appropriate FIU and make relevant transaction information available to the FIU. The lack of required originator or beneficiary information should be considered as a factor in assessing whether a transfer involving VAs or VASPs is suspicious and whether it is thus required to be reported to the FIU. The same holds true for other obliged entities such as traditional FIs involved in a transfer involving VAs or VASPs.

SECTION V – COUNTRY EXAMPLES OF RISK-BASED APPROACH TO VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS

Summary of Jurisdictional Approaches to Regulating and Supervising VA Activities and VASPs

196. Section V provides an overview of various jurisdictional approaches to regulating and supervising VA financial activities and related providers, including approaches to having in place tools and other measures for sanctioning or taking enforcement actions against persons that fail to comply with their AML/CFT obligations, which countries might consider when developing or enhancing their own national frameworks. These countries have not yet been assessed for their compliance with the requirements set forth in INR. 15.

Italy

197. In Italy, Decree No. 231 of 2007, amended by Legislative Decree No. 90 of 2017, includes providers engaged in exchange services between VA and fiat currencies (*i.e.*, “virtual currency exchangers”) within the category of subjects obliged to comply with the AML/CFT requirements.

198. Service providers related to VAs are required to be listed in a special section of the register held by “*Organismo degli Agenti e dei Mediatori*” (OAM). The registration is a precondition for service providers related to VAs in order to carry out their activity in Italy. Work is currently ongoing to implement the register.

199. VASPs are considered obliged entities and are subject to the full set of AML/CFT measures.

200. On March 21, 2019, Italy adopted the update of the National Risk Assessment (NRA). It includes an assessment of the ML/TF risks emanating from VAs. The results of the updated NRA will be used in order to strengthen the national strategy. Obligated entities and subjects (financial and non-financial) are requested to take into consideration the results of the updated NRA in order to conduct/update their risk assessment.

201. The STRs and the further analysis conducted by the Italian FIU (UIF) permit it to collect information about: i) VASPs operating in Italy, including business data (typology of service provided); location; data on the beneficial owner, administrator and other connected subjects; ii) detailed information on single transactions (*e.g.*, date, amount, executor, counterparts, and wallet accounts); data on the bank accounts involved (*e.g.*, holder, power of attorney, origin/use of the funds, and general features of the financial flows); iii) data on the personal and economic profile of the customer or the holder of the wallet; information useful to match VA addresses to the identity of the owner of the VAs; unambiguous identification data (*e.g.*, fiscal code and VAT number); iv) wallet or account information (*e.g.*, overall amount of VAs owned by one or more subjects; detailed information on main movements of VAs traced back to the same subject or linked subjects in a specific timeframe; wallet/account statement in an editable format; and v) type and main features of VAs.

202. Since 2015, the Bank of Italy has warned consumers on the high risks of buying and/or holding VAs as well as supervised financial intermediaries about the possible risks associated with VAs. In particular, it issued a warning for consumers and a communication for supervised financial intermediaries (January 2015) as well as a new warning for consumers which recalled the one issued by the three European financial authorities—European Securities and Markets Authority (ESMA), the European Banking Authority (EBA), and the European Insurance and Occupational Pensions Authority (EIOPA) in March 2018. The Italian UIF, in order to enhance the engagement with the private sector, issued a Communication on January 30, 2015 about the anomalous use of crypto-assets, addressing particularly the financial

institutions (*i.e.*, banks and payment institutions) as well as gambling operators, and underlining the necessity for these obliged entities to focus their attention on possible anomalous transactions, such as wire transfers, cash deposits and withdrawals, use of prepaid cards, associated with crypto-assets purchases or investments.

203. The UIF is progressing its analysis, focussing on new risks and emerging trends. An updated Communication was issued in 2019 to assist obliged entities in performing their tasks. In particular, the UIF updated its 2015 Communication on the anomalous use of crypto-assets by providing more details on recurring elements, operational methods, and behavioral risk profiles identified in STRs related to VAs. The Communication sets out specific instructions for filling in data in the pre-set STRs' format, particularly with reference to information about: VASPs, transactions, users/customers, and wallets/accounts.
204. In December 2016 and July 2018, the UIF published collections of sanitized cases of money laundering and terrorist financing that emerged in the course of financial analyses, including typologies connected to the anomalous use of VAs.

Norway

205. VASPs have been subject to the Norwegian AML Act and its obligations since October 15, 2018. The relevant provision of the AML regulation reads as follows:

Section 1-3 Application of the Anti-Money Laundering Act to Virtual Currency

(1) Providers of exchange services between virtual currency and official currency are obliged entities within the meaning of the Anti-Money Laundering Act. This shall apply correspondingly to virtual currency custodianship services.

(2) By virtual currency is meant a digital expression of value, which is not issued by a central bank or a government authority, which is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but which is accepted as a means of exchange, and which can be transferred, stored or traded electronically.

(3) By virtual currency custodianship services is meant the custodianship of private cryptographic keys on behalf of customers, for purposes of transferring, storing or trading in virtual currency.

(4) The Financial Supervisory Authority may supervise compliance with the Anti-Money Laundering Act for the providers mentioned in paragraph 1. Providers as mentioned in paragraph 1, shall be registered with the Financial Supervisory Authority. The following information shall be registered on the provider:

- a) name
- b) type of enterprise and organisation number
- c) business address
- d) the service which is offered
- e) name, residence address and personal identity number or D number on the

- i) general manager or persons in a corresponding position
- ii) members of the board of directors or persons in a corresponding position
- iii) any other contact person

206. As of June 2019, six VAPs have been registered, and more than 20 other VASPs have applied for registration, but have applications pending due to shortcomings in their AML policies and procedures. Three VA ATMs have been shut down in November 2018 after cease and desist orders from the FSA, and no new ATMs have been set up since. The FSA will commence inspections of the sector, but based on the registration applications in the second half of 2019, it is clear that the field of VASPs registered, and attempting to register, includes a range of actors with differences in size, competence, knowledge of AML rules, and professionalism.

Sweden

207. In Sweden, the Financial Supervisory Authority has considered bitcoin and ethereum as means of payment since 2013, meaning that professional exchange services are therefore subject to a licensing regime²⁶ and, following a successful application for a licence, AML/CFT supervision. The regulation is not an explicit AML/CFT regulation of VA exchange services as such (*i.e.*, they are not specifically mentioned in the law) but an implicit recognition that they should be regulated. Once an exchange service obtains a licence, all activities (*i.e.*, no matter the VA in question) are subject to AML/CFT regulation and supervision. Thematic supervision has been carried out. As a result, part of the sector has ceased its operations. VASPs have submitted STRs to the FIU, and feedback from operational authorities suggests that criminals are choosing to take their business to unregulated exchanges elsewhere.

Finland

208. The Act on Virtual Currency Providers (572/2019) came into force on May 1st 2019. VASPs are required to register (authorization) with the Finnish Financial Supervisory Authority (FIN-FSA).²⁷ Those who already provided services before legislation came into force, need to be registered by November 1st 2019. New actors have to be registered prior to starting their operations. The definition of VASPs includes exchanges (both fiat to VAs and between VAs as well as VAs and other goods such as gold), custodian wallet providers, and ICOs. The requirements for registration include basic fit and proper checks, requirements for handling customer funds, and simple rules regarding marketing (*i.e.*, an obligation to give all relevant information and an obligation for truthful information). VASPs are obliged entities as defined in the AML Act (444/2017) and are required to comply with AML/CFT obligations from December 1st 2019. VASP's AML/CFT risk assessment and their procedures and guidelines relating to AML/CFT are reviewed as part of the registration process.

209. FIN-FSA was given powers to issue regulations and guidance on certain parts of VASP activity. FIN-FSA draft regulation was published for consultation on May 21st. The draft contains regulation on holding and protecting client money and segregation of client money and own

²⁶ It is not quite a comprehensive licensing regime in the prudential sense of the word, but for AML/CFT purposes it is, including fit and proper testing of owners and management and an assessment of whether the business will be conducted pursuant to AML/CFT regulation.

²⁷ www.finanssivalvonta.fi/en/banks/fintech--financial-sector-innovations/virtuaalivaluutan-tarjoajat/

funds. Guidance is given on compliance with AML/CFT regulation. The aim is to publish the regulation during summer.

210. Prior to the Act, the FIN-FSA has been working with organizers of ICOs from the point of view of securities markets legislation and financial instruments. The aim has been to identify when the VA is a financial instrument (*i.e.*, transferable security). For this purpose, the FIN-FSA has drafted a checklist that is used in all ICO-related enquiries. The checklist as well as frequently asked questions related to VAs are available at the FIN-FSA website.²⁸
211. The FIN-FSA supervisory experience has shown that VASPs are now willing and keen on being regulated and trying to seek supervisors' endorsement for their activities. The challenge is to communicate to the general public that authorization does not equal endorsement. FIN-FSA has seen a total turn in VASPs attitude towards regulation. Some time ago they did not want to be regulated, but now they are seeking business models through which they could be regulated. VASPs have had challenges in opening bank accounts, which could partly explain the change in their attitude towards regulation.

Mexico

212. In Mexico, Federal Law *for the Prevention and Identification of Operations with Resources of Illegal Proceeds* was reformed in March 2018 to establish as a *Vulnerable Activity* the exchange of VAs made by entities other than Financial Technology Institutions and Credit Institutions.
213. Likewise, in March 2018, Mexico published the *Law to Regulate Financial Technology Institutions*, which indicates that Financial Technology Institutions may operate with VAs provided that they have the authorization of Bank of Mexico and operate with the VA that it determinates.
214. Subsequently, in September 2018, the standards that establish the measures and procedures in terms of AML/CFT related to VAs were published.
215. In March 2019, the Central Bank published the standards to define the internal operations that the Credit Institutions and the Financial Technology Institutions directly or indirectly pretend to carry out operations with VA.
216. The Central Bank said that VAs carry a significant ML/TF risk, due to the ease of transferring VA to different countries as well as the absence of homogeneous controls and prevention measures at the global level. However, it seeks to promote the use of technologies that could have a benefit, as long as these technologies are used internally between Financial Technology Institutions and Credit Institutions.
217. Finally, later in March 2019, the *Disposiciones de carácter general a que se refiere el Artículo 115 de la Ley de Instituciones Crédito* were reformed, establishing the measures and procedures that the credit institutions must follow to comply with the obligations regarding AML/CFT related to VAs.

Japan

218. Japan amended the *Payment Services Act and Act on Prevention of Transfer of Criminal Proceeds* (PTCP Act) in 2016 in response to the bankruptcy of a large VASP in 2014 and the 2015 FATF VC Guidance. Following the enactment of the laws in April 2017, the JFSA established a VASP monitoring team in August 2017, composed of AML/CFT and technology specialists.

²⁸. www.finanssivalvonta.fi/en/banks/fintech--financial-sector-innovations/virtuaalivaluutan-tarjoajat/frequently-asked-questions-on-virtual-currencies-and-their-issuance-initial-coin-offering/

219. As a part of its registration procedure, the JFSA assesses applicants' AML/CFT programs, with a focus on consistency between the applicants' risk assessment and their business plan, through document-based assessment and off-site or on-site interviews with them (as of March 2019, 19 VASPs are registered).
220. The JFSA imposes a periodical report-submission order on VASPs to seek quantitative and qualitative information on inherent risk and controls. The JFSA utilizes the collected information for its own risk assessment and monitoring of VASPs. The JFSA has conducted on-site inspections of 22 VASPs (including 13 then-deemed VASPs, *i.e.*, entities which were already in business before the enactment of the amended act, being allowed to operate on a tentative basis) and has imposed administrative dispositions (21 business improvement orders and six business termination orders and one refusal of registration) by March 2019.
221. The JFSA also closely co-operates with the Japan Virtual Currency Exchange Association (JVCEA), the self-regulatory body certified in October 2018, for prompt and flexible response to VASP-related issues. The JVCEA functions as an educational body and a monitoring body for the member VASPs. Compliance with self-regulatory AML/CFT rules and guidelines is prepared by the JVCEA. The JFSA, in consultation with the JVCEA, has conducted outreach, some of which was done in collaboration with other authorities, sharing information and ideas with VASPs that would contribute to improving their AML/CFT compliance.
222. In addition, the JFSA:
 - Established the “*Study Group on the Virtual Currency Exchange Business*” in March 2018 to examine institutional responses to various issues related to the VASP business. In light of suggestions made on a report compiled by the Group, the JFSA, in March 2019, submitted to the Diet a bill to amend the acts. The amendment includes: the application of the Payment Services Act and PTCP Act to service providers who conduct custodian service of VAs; and the introduction of *ex ante* notification system concerning each change of a type of VA dealt in by VASPs taking into account the anonymity of VAs.
 - Prepared and publicized red flag indicators of suspicious transactions, which are specific to VASPs, in April 2019. The indicators cover several transactions where anonymization technology was utilized.

United States

Comprehensive and Technology-Neutral Framework

223. The United States has a comprehensive and technology-neutral regulatory and supervisory framework in place for regulating and supervising “digital financial assets”²⁹ for AML/CFT that subjects covered providers and activities in this space to substantially the same regulation that providers of non-digital assets are subject to within the existing AML/CFT regulatory framework for U.S. financial institutions. The U.S. approach draws on the tools and authorities of various departments and agencies, including the U.S. Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN), the U.S. FIU and administrator of the primary U.S. AML law, the Bank Secrecy Act (BSA); U.S. Treasury’s Office of Foreign Assets Control (OFAC); the

²⁹ From a U.S. perspective, the term “digital financial assets” (or “digital assets”) is a comprehensive term that refers to a range of activities in the digital financial services ecosystem, including financial activities involving digital currencies—both national digital currencies and digital currencies that are not issued or guaranteed by a national government, such as digital forms of convertible virtual currencies like bitcoin—as well as digital securities, digital commodities, or digital derivatives thereof.

Internal Revenue Service (IRS); the U.S. Securities and Exchange Commission (SEC); the U.S. Commodity Futures Trading Commission (CFTC); and other departments and agencies. FinCEN, the IRS, the SEC, and the CFTC in particular have regulatory, supervisory, and enforcement authorities to oversee certain digital asset activities that involve money transmission; securities, commodities, or derivatives; or that have tax implications, and they have authority to mitigate the misuse of digital assets for illicit financial transactions or tax avoidance.

224. Where a person (a term defined in U.S. regulation that goes beyond natural and legal persons) engages in certain financial activities involving digital assets, AML/CFT and other obligations apply. Depending on the activity, the person or institution is subject to the supervisory authority of FinCEN, the SEC, and/or the CFTC to regulate the person as a money transmitter, national securities exchange, broker-dealer, investment adviser, investment company, transfer agent, designated contract market, swap execution facility, derivatives clearing organization, futures commission merchant, commodity pool operator, commodity trading advisor, swap dealer, major swap participant, retail foreign exchange dealer, or introducing broker.
225. If the person falls under the regulatory definition of a “bank,” FinCEN and the U.S. federal banking agencies—the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, and National Credit Union Administration—have authority, sometimes concurrent with that of the state banking regulators, to regulate and supervise persons when they engage in financial activity involving digital assets. Moreover, existing general tax principles apply to transactions involving digital assets in the United States because the IRS classifies them as property.

Case Study: U.S. Regulation and Supervision (Including Licensing and Registration) of Digital Asset-Related Providers

Money Transmission. At the federal level, FinCEN regulates as money transmitters any person engaged in the business of accepting and transmitting value, whether physical or digital, that substitutes for currency (including convertible virtual currency, whether virtual-to-virtual, virtual-to-fiat, or virtual-to-other value) from one person to another person or location by any means. Under the BSA, money transmitters must register with FinCEN as money services businesses and institute AML program, recordkeeping, and reporting measures, including filing suspicious activity reports. The AML requirements apply equally to domestic and foreign-located money transmitters, even if the foreign-located entity does not have a physical presence in the United States and regardless of where it is incorporated or headquartered, as long as it does business in whole or substantial part in the United States. Since 2014, the IRS and FinCEN have conducted examinations of various digital asset-related providers, including administrators, some of the largest exchangers by volume, individual peer-to-peer exchangers, foreign-located exchangers, digital asset/crypto-precious metal dealers, kiosk companies, and numerous trading platforms as well as registered and unregistered financial institutions. Applicable state laws also require relevant covered entities to obtain state money transmitter licenses in most states in which they operate, regardless of their jurisdiction of incorporation or the physical location of their head office. Money transmitters also may be subject to

other regulatory requirements, including safety, soundness, and capital reserve requirements, depending on the U.S. state in which they are located or do business and whether or not their operations make them subject to the rules of other U.S. regulatory bodies.

Securities Activity. To the extent a digital asset is a security in the United States, the SEC has regulatory and enforcement authority that extends to the offer, sale, and trading of, and other financial services and conduct relating to, those digital assets. Platforms on which digital assets that are securities are traded in the secondary market generally must register as national securities exchanges or operate pursuant to an exemption from registration, such as the exemption under SEC requirements for alternative trading systems (*i.e.*, SEC Regulation ATS), and report information about their operations and trading to the SEC. Even if the securities exchange, broker-dealer, or other similar securities-related entity is a foreign-located person and does not have a physical presence in the United States, the person may be subject to SEC regulations and jurisdiction when they offer, sell, or issue securities (including, potentially, certain ICO tokens) to U.S. persons or investors or otherwise affect the U.S. securities markets. Additional state licensing obligations may apply depending on the activity in which an entity is engaged and on the state in which the activity is conducted. Certain trading in digital assets, including trading on platforms, may still qualify as money transmission under the BSA and state laws or regulations, as discussed above. If the digital asset is a security, it is subject to SEC jurisdiction and any derivative on the security is subject to SEC jurisdiction.

Commodities and Derivatives Activity. In the United States, digital assets may also qualify as commodities or derivatives thereof, even if not a security, in which case persons dealing in such digital assets are subject to CFTC jurisdiction. The CFTC has full regulatory authority over derivatives on digital assets that are not securities (*e.g.*, futures contracts). The CFTC exercises anti-fraud and anti-manipulation regulatory authority over the sale of such assets and requires registration in connection with trading in futures or certain other derivatives on such commodities. Pursuant to the Commodity Exchange Act and related Regulations, the CFTC has broad authority to take action against any person or entity located inside or outside the United States that is associated with or engaged in fraud or manipulative activity (*e.g.*, U.S. CFTC *v.* Blue Bit Banc).

Generally, a natural or legal person that transacts in securities, commodities or derivatives is subject to additional oversight by a self-regulatory organization. Securities activities require registration with the Financial Industry Regulatory Authority (FINRA), and commodities and derivatives activities require registration with the National Futures Association (NFA). Depending on its activities, a natural or legal person may also require dual registration with FINRA and the NFA, both of which have statutory obligations under U.S. federal securities and commodities laws. Additionally, similar to money transmitter licenses, a natural or legal

person must be licensed with each state regulatory for states in which they do business.

Certain registrants of the SEC and CFTC also have BSA obligations, including establishing AML programs, reporting suspicious activity to FinCEN, identifying and verifying customer identity, and applying enhanced due diligence for certain accounts involving foreign persons. The relevant regulatory and supervisory bodies also monitor digital asset activities and examine registrants for compliance with their regulatory obligations, including (for certain registrants) AML/CFT obligations under the BSA.

U.S. Law Enforcement, Sanctions, and Other Enforcement Capabilities

226. U.S. law enforcement uses financial intelligence information from FinCEN to conduct investigations involving digital assets. Such information—which is sourced from the reporting and analysis that FinCEN collects and disseminates to competent U.S. law enforcement authorities—has been useful in developing evidence of criminal activity and identifying individuals who may be involved in ML or TF activities. FinCEN has access to a wide range of financial, administrative, and law enforcement information. The information at FinCEN’s disposal includes two key pieces of information that can be instrumental in detecting suspected ML or TF involving digital assets: (i) suspicious activity reports (or STRs) filed by traditional reporting financial institutions, such as banks or broker-dealers in securities for example, that have transmitted fiat currency for conversion or exchange into a digital asset at a digital asset exchanger or related business or that have received fiat currency from a digital asset exchanger or related business after being converted or exchanged from a digital asset; and (ii) suspicious activity reports filed by digital asset providers that, as money transmitters, receive funds and convert them into a digital asset or allow for the storage and/or trading and exchange of digital assets. FinCEN also collects foreign bank account, currency and monetary instrument, and currency transaction reports—all of which could contain investigative leads and evidence necessary to deter and prosecute criminal activity associated with digital assets.
227. U.S. departments and agencies have taken strong civil and criminal enforcement actions in both administrative proceedings and federal court to combat illicit activity relating to digital assets, such as by seeking various forms of relief, including cease and desist orders, injunctions, disgorgement with prejudgment interest, and civil money penalties for wilful violations and imposing criminal sentences involving forfeiture and imprisonment.³⁰ U.S. regulators and supervisors engage extensively with one another, state regulators, the U.S. Department of Justice (DOJ), and other law enforcement agencies to support investigative and prosecutorial efforts in the digital assets space.
228. A variety of criminal and civil authorities, policy tools, and legal processes exist to assist U.S. government agencies in identifying illicit digital asset-related activity, attributing transactions to a specific individual or organization, mitigating threats, and performing analysis relating to their respective regulatory or criminal investigative functions. For such investigations and prosecutions, DOJ relies on a range of statutory criminal and civil authorities, including federal

³⁰ *Select examples of U.S. enforcement, investigative, and/or sanctions actions include:* 2015 civil money penalty against [Ripple Labs, Inc.](#); 2016 [Operation Dark Gold](#); 2017 civil money penalties against [BTC-e](#) and concurrent indictment of [Alexander Vinnik](#); 2017 TF case, [U.S. v. Zoobiq Shahnaz](#); 2018 sentencing of [unlicensed bitcoin trader](#); and 2019 identification of digital currency addresses associated with [OFAC SamSam designation](#).

laws governing money laundering, money services businesses registration, financial institution recordkeeping and reporting requirements, fraud, tax evasion, the sale of controlled substances and other illegal items and services, computer crimes, and terrorist financing. The United States has charged and prosecuted individuals operating as peer-to-peer exchangers for violating the BSA or money laundering as well as foreign-located persons and organizations who violate U.S. law, among other prosecutions relating to digital assets.

229. Similar to FinCEN, SEC, and CFTC authorities, DOJ has broad authority to prosecute digital asset providers and individuals who violate U.S. law, even though they may not be physically located inside the United States. Where digital asset transactions touch financial, data storage, or other computer systems within the United States, for example, the DOJ has jurisdiction to prosecute persons directing or conducting those transactions. The United States also has jurisdiction to prosecute foreign-located persons who use digital assets to import illegal products or contraband into the United States or who use U.S.-located digital asset businesses or providers or financial institutions for money laundering purposes. In addition, foreign-located persons who provide illicit services to, defraud, or steal from U.S. residents may be prosecuted for violations of U.S. law.
230. OFAC, typically in consultation with other agencies, administers U.S. financial sanctions and associated licensing, regulations, and penalties, all of which relate to digital assets as well as most other types of assets. OFAC has made clear that U.S. sanctions compliance obligations are the same, regardless of whether a transaction is denominated in digital currency (whether national digital currency or non-national digital currency such as convertible virtual currency like bitcoin) or traditional fiat currency, and U.S. persons and persons otherwise subject to OFAC jurisdiction are responsible for ensuring they do not engage in unauthorized transactions prohibited by OFAC sanctions.

International Co-operation is Key

231. The inherently global nature of the digital asset ecosystem makes digital asset activities particularly well suited for carrying out and facilitating crimes that are transnational in nature. Customers and services can transact and operate with little regard to national borders, creating jurisdictional hurdles. Effectively countering criminal activity involving digital assets requires close international partnerships.
232. U.S. departments and agencies, particularly U.S. law enforcement, work closely with foreign partners in conducting investigations, making arrests, and seizing criminal assets in cases involving digital asset activity. The United States has encouraged these partnerships to support multi-jurisdictional investigations and prosecutions, particularly those involving foreign-located persons, digital asset providers, and transnational criminal organizations. Mutual legal assistance requests remain a key mechanism for enhancing co-operation. Because illicit actors can quickly destroy, dissipate, or conceal digital assets and related evidence, the United States has developed policies for obtaining evidence and restraining assets located abroad, recognizing that digital assets and the associated transactional data and evidence may be stored or located via technological means and processes not contemplated by current legal methods and treaties.

Annex A. Recommendation 15 and its Interpretive Note and FATF Definitions

Recommendation 15 – New Technologies

Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.

Interpretative Note to Recommendation 15

1. For the purposes of applying the FATF Recommendations, countries should consider virtual assets as “property,” “proceeds,” “funds,” “funds or other assets,” or other “corresponding value.” Countries should apply the relevant measures under the FATF Recommendations to virtual assets and virtual asset service providers (VASPs).
2. In accordance with Recommendation 1, countries should identify, assess, and understand the money laundering and terrorist financing risks emerging from virtual asset activities and the activities or operations of VASPs. Based on that assessment, countries should apply a risk-based approach to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. Countries should require VASPs to identify, assess, and take effective action to mitigate their money laundering and terrorist financing risks.
3. VASPs should be required to be licensed or registered. At a minimum, VASPs should be required to be licensed or registered in the jurisdiction(s) where they are created.¹ In cases where the VASP is a natural person, they should be required to be licensed or registered in the jurisdiction where their place of business is located. Jurisdictions may also require VASPs that offer products and/or services to customers in, or conduct operations from, their jurisdiction to be licensed or registered in this jurisdiction. Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a VASP. Countries should take action to identify natural or legal persons that carry out VASP activities without the requisite license or registration, and apply appropriate sanctions.
4. A country need not impose a separate licensing or registration system with respect to natural or legal persons already licensed or registered as financial institutions (as defined by the FATF Recommendations) within that country, which, under such license or registration, are permitted to perform VASP activities and which are already subject to the full range of applicable obligations under the FATF Recommendations.
5. Countries should ensure that VASPs are subject to adequate regulation and supervision or monitoring for AML/CFT and are effectively implementing the relevant FATF Recommendations, to mitigate money laundering and terrorist financing risks emerging from virtual assets. VASPs should be subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements. VASPs should be supervised or monitored

- by a competent authority (not a SRB), which should conduct risk-based supervision or monitoring. Supervisors should have adequate powers to supervise or monitor and ensure compliance by VASPs with requirements to combat money laundering and terrorist financing including the authority to conduct inspections, compel the production of information, and impose sanctions. Supervisors should have powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the VASP's license or registration, where applicable.
6. Countries should ensure that there is a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with VASPs that fail to comply with AML/CFT requirements, in line with Recommendation 35. Sanctions should be applicable not only to VASPs, but also to their directors and senior management.
 7. With respect to preventive measures, the requirements set out in Recommendations 10 to 21 apply to VASPs, subject to the following qualifications:
 - (a) R.10 – The occasional transactions designated threshold above which VASPs are required to conduct CDD is USD/EUR 1 000.
 - (b) R.16 – Countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information² on virtual asset transfers, submit³ the above information to the beneficiary VASP or financial institution (if any) immediately and securely, and make it available on request to appropriate authorities. Countries should ensure that beneficiary VASPs obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers, and make it available on request to appropriate authorities. Other requirements of R.16 (including monitoring of the availability of information, and taking freezing action and prohibiting transactions with designated persons and entities) apply on the same basis as set out in R.16. The same obligations apply to financial institutions when sending or receiving virtual asset transfers on behalf of a customer.
 8. Countries should rapidly, constructively, and effectively provide the widest possible range of international co-operation in relation to money laundering, predicate offences, and terrorist financing relating to virtual assets, on the basis set out in Recommendations 37 to 40. In particular, supervisors of VASPs should exchange information promptly and constructively with their foreign counterparts, regardless of the supervisors' nature or status and differences in the nomenclature or status of VASPs.
 - ¹ References to creating a legal person include incorporation of companies or any other mechanism that is used.
 - ² As defined in INR. 16, paragraph 6, or the equivalent information in a virtual asset context.
 - ³ The information can be submitted either directly or indirectly. It is not necessary for this information to be attached directly to virtual asset transfers.

FATF Glossary

A **virtual asset** is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.

Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- i) exchange between virtual assets and fiat currencies;
- ii) exchange between one or more forms of virtual assets;
- iii) transfer¹ of virtual assets;
- iv) safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
- v) participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

¹ In this context of virtual assets, transfer means to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another.

FATF



12-MONTH REVIEW OF THE REVISED FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS



JUNE 2020

Appendix F



The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit www.fatf-gafi.org

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2020), *12-month Review Virtual Assets and VASPs*, FATF, Paris, France,
www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html

© 2020 FATF/OECD. All rights reserved.

No reproduction or translation of this publication may be made without prior written permission.

Applications for such permission, for all or part of this publication, should be made to the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France (fax: +33 1 44 30 61 37 or e-mail: contact@fatf-gafi.org)

Photocredits coverphoto ©Gettyimages

Table of Contents

Executive summary	2
Introduction	3
12-month review	4
Section 1: ML/TF risks and the virtual asset market	6
Trends in use of virtual assets for ML/TF purposes	6
Trends in virtual asset market structure	7
Section 2: State of implementation by the public sector	8
Section 3: State of implementation by the private sector	11
Implementation of the travel rule	11
Implementation of other AML/CFT obligations	12
Section 4: Issues identified with the revised FATF Standards and Guidance	14
Definition of virtual asset and VASP	14
Peer-to-peer transactions and private / non-custodial wallets	14
So-called stablecoins	15
Identifying VASPs for registration / licencing	16
Travel rule implementation	16
Section 5: Proposed next steps	19
Annex A. Recommendation 15 and its Interpretive Note and FATF Definitions	21
Recommendation 15 – New Technologies	21
Interpretative Note to Recommendation 15	21
FATF Glossary	23
References	24

Executive summary

1. The Financial Action Task Force (FATF) is the inter-governmental body which sets international standards to prevent money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction. In June 2019, the FATF finalised amendments to its global Standards to clearly place anti-money laundering and counter-terrorism financing (AML/CFT) requirements on virtual assets and virtual asset service providers (VASPs). The FATF agreed to establish a Virtual Assets Contact Group to promote implementation, identify issues and engage with the private sector to monitor progress. The FATF also agreed to undertake a 12-month review to measure the implementation of the revised Standards by jurisdictions and the private sector, as well as monitoring for any changes in the typologies, risks and the market structure of the virtual assets sector.

2. This report sets out the findings of this review. The report finds that, overall, both the public and private sectors have made progress in implementing the revised FATF Standards. 35 out of 54 reporting jurisdictions advised that they have now implemented the revised FATF Standards, with 32 of these regulating VASPs and three of these prohibiting the operation of VASPs. The other 19 jurisdictions have not yet implemented the revised Standards in their national law. While the supervision of VASPs and implementation of AML/CFT obligations by VASPs is generally nascent, there is evidence of progress. In particular, there has been progress in the development of technological solutions to enable the implementation of the ‘travel rule’¹ for VASPs, even though there remain issues to be addressed by the public and private sectors.

3. At this stage in time, there is no clear need to amend the revised FATF Standards. This review has not identified any fundamental issues that would require amending the revised Standards. Nonetheless, there is still a substantial amount of work to be done. While more than half of reporting jurisdictions advised that they have introduced AML/CFT regimes for VASPs, all FATF members and its broader Global Network of nine FATF-Style Regional Bodies (FSRBs) and their respective members must implement the revised FATF Standards. The effectiveness of the revised FATF Standards is contingent on all jurisdictions implementing the revised FATF Standards and the private sector implementing their AML/CFT obligations. The feedback from the public and private sectors also indicates that there is a need for greater FATF Guidance on how to implement the revised FATF Standards. This could include tailored guidance for low-capacity jurisdictions.

4. The virtual asset sector is fast-moving and technologically dynamic, which means continued monitoring and engagement between the public and private sectors is necessary. At the same time, the one-year timeframe of this review has proved to be a relatively short time period to fully understand the impact of the revised FATF Standards and how the virtual asset market has changed. Accordingly, the FATF has agreed to continue its focus on virtual assets and undertake the following actions. The FATF will:

- a) continue its enhanced monitoring of virtual assets and VASPs and undertake a second 12-month review of the implementation of the revised FATF Standards on virtual assets and VASPs by June 2021. By this time, jurisdictions

¹ The ‘travel rule’ is a key AML/CFT measure, which mandates that VASPs obtain, hold and exchange information about the originators and beneficiaries of virtual asset transfers.

will have had two years to transpose the revised FATF Standards on VASPs into law and the VASP sector will have had time to implement travel rule solutions globally;

- b) release updated Guidance on virtual assets and VASPs;
 - c) continue to promote the understanding of ML/TF risks involved in transactions using virtual assets and the potential misuse of virtual assets for ML/TF purposes by publishing red flag indicators and relevant case studies by October 2020;
 - d) continue and enhance its engagement with the private sector, including VASPs, technology providers, technical experts and academics, through its Virtual Assets Contact Group; and
 - e) continue its program of work to enhance international co-operation amongst VASP supervisors.
5. As set out in this report, these actions set the FATF's forward work program on virtual assets for the coming year. These findings also support the conclusions made by the FATF in its report to the G20 on so-called stablecoins.

Introduction

6. The emergence of new technologies, products and related services over the last decade has been one of the major changes to the global financial system. These new technologies, products, and related services have the potential to spur financial innovation and efficiency and improve financial inclusion, but they also create new opportunities for criminals and terrorists to launder their proceeds or finance their illicit activities. Consistent with the risk-based approach which underpins the FATF Standards, understanding and responding to identified money laundering and terrorist financing (ML/TF) risks is at the heart of what the FATF does. The FATF is the inter-governmental body which sets the international standards to prevent money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction.

7. In June 2014, the FATF issued [Virtual Currencies: Key Definitions and Potential AML/CFT Risks](#) in response to the emergence of virtual currencies and their associated payment mechanisms. In June 2015, the FATF issued the [Guidance for a Risk-Based Approach to Virtual Currencies](#) as part of a staged approach to addressing the ML/TF risks associated with virtual currency payment products and services.

8. As the virtual asset market continued to evolve and develop, the FATF recognized the need for further clarification on the application of the FATF Standards to virtual assets and their service providers. In October 2018, the FATF adopted two new Glossary definitions – “virtual asset” and “virtual asset service provider” (VASP) – and updated Recommendation 15 (R.15). Virtual assets is the term the FATF uses to refer to crypto-assets and other digital assets. In June 2019, the FATF adopted an Interpretive Note to Recommendation 15 (INR.15) to further clarify how the FATF requirements apply in relation to virtual assets and VASPs (see **Annex A**). These changes were accompanied by a new [Guidance for a Risk-Based Approach for Virtual Assets and VASPs](#). Finally, in October 2019 the FATF updated its [Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems](#) to reflect the revised Standards.

Changes to FATF Standards	Changes to FAT Methodology	Changes to FATF Guidance
<ul style="list-style-type: none"> • New definitions of 'virtual asset' and 'virtual asset service provider' • Revised R.15 • New INR.15 	<ul style="list-style-type: none"> • New definitions of 'virtual asset' and 'virtual asset service provider' • Technical compliance - Revised R.15 • Effectiveness - Revised methodology, particularly Immediate Outcomes 3 and 4 	<ul style="list-style-type: none"> • Release of new FATF Guidance on a Risk-Based Approach for virtual assets and VASPs

12-month review

9. When the FATF finalised the revisions to the FATF Standards in June 2019, the FATF also agreed to undertake a 12-month review of the changes, to be completed by June 2020. The FATF also agreed to establish a Virtual Assets Contact Group to promote implementation, identify issues and engage with the private sector to monitor progress. The scope of the review is as follows:

- a) *Monitoring jurisdictions' implementation of the new requirements by FATF and FSRB members.* The review would consider whether jurisdictions have transposed the requirements into law and regulation, established supervisors or implemented other regulatory framework changes, and implemented licensing/registering requirements for VASPs, among other obligations under the FATF Recommendations.
- b) *Monitoring VASPs' (as well as other obliged entities') progress in developing and implementing their obligations under the FATF Recommendations,* including in the context of any related technology solutions or communications protocols.
- c) *Monitoring the VASP sector for any potential changes in typologies, risks and the market structure of the sector.* The review would seek to give the FATF early indications of emerging risks and typologies involving virtual assets.

10. Information on these issues has informed the analysis below on whether the revised FATF Standards, particularly R.15 and INR.15, should be adjusted, whether future updated Guidance is warranted and whether jurisdictions and the private sector are making progress in implementing the revised Standards. This review has not assessed individual jurisdiction's compliance with the revised FATF Standards.

11. The following information sources have informed the review:

- a) A questionnaire surveying jurisdictions' implementation was conducted in March 2020. 38 FATF members (37 jurisdictions and 1 regional organisation) and 16 FSRB member jurisdictions responded to the questionnaire or provided updates on their progress. It should be noted that the questionnaire was a self-assessment by participating jurisdictions and is not an official FATF assessment of the level of implementation by jurisdictions.
- b) Outreach to representatives from the VASP sector through meetings with the Virtual Assets Contact Group in February and April 2020. These meetings have included a select number of VASPs, industry associations and technology

providers, but cannot be taken to represent the views of the entirety of the global VASP sector.

- c) The results from the completed follow-up reports using the revised FATF Standards (the United States of America² and Switzerland³).
 - d) The findings from the FATF's report to the G20 on so-called stablecoins.⁴
 - e) The findings from the FATF's ongoing work to understand the ML/TF risk environment and to review ML/TF cases involving virtual assets.
 - f) Desk-based research by the Secretariat into trends and market metrics involving virtual assets.
12. This report sets out the findings of this review as follows:
- a) Section 1 sets out how ML/TF risks and the virtual asset market have changed since June 2019;
 - b) Section 2 sets out jurisdictions' progress in implementing the revised Standards;
 - c) Section 3 sets out the private sector's progress in implementing the revised Standards, including the development of technical solutions for the implementation of the travel rule;
 - d) Section 4 sets out issues identified with the revised FATF Standards and Guidance; and
 - e) Section 5 sets out the FATF's next steps.

² FATF, [United States: 2nd Enhanced Follow-up Report and Technical Compliance Re-Rating](#), March 2020

³ FATF, [Switzerland: 2nd Enhanced Enhanced Follow-up Report and Technical Compliance Re-Rating](#), January 2020

⁴ FATF, [Report to G20 on so-called stablecoins](#), June 2020

Section 1: ML/TF risks and the virtual asset market

13. This section sets out how the ML/TF risks and the virtual asset market has changed since June 2019. This section is based on information collected by FATF through its regular collection of virtual asset case studies, information collected through the questionnaire and desk-based research by the Secretariat.

14. As the revisions to the FATF Standards were only finalised in June 2019, it remains early to assess whether the revised Standards have resulted in changes to the typologies, ML/TF risks and the market structure of the virtual assets sector. This is not only because this is a short period of time, but because the FATF Standards are reliant on jurisdictions transposing the Standards into their national law and operationalising these laws. As set out in Section 2, some jurisdictions are still in the process of implementing the revised FATF Standards.

15. In addition, the virtual asset market is fast-moving and quickly evolving. The usage of virtual assets and VASPs is constantly changing, as products and services enter and leave the market and the sector as a whole matures. Changes in the usage of a particular virtual asset or VASP could be driven by a range of factors. These factors include consumer preferences, competition, regulation, speculation, technological development and privacy and security concerns. This makes it very difficult to directly link the revisions to the FATF Standards to any changes in the virtual asset and VASP market in the short time period. A longer time period may illuminate more concrete or obvious trends in the market or ML/TF risk profile. Nevertheless, this Section sets out the FATF's observations of trends since June 2019.

Trends in use of virtual assets for ML/TF purposes

16. The FATF has observed the following trends on the use of virtual assets for ML/TF purposes. The value of virtual assets involved in most ML/TF cases detected to date has been relatively small so far compared to cases using more traditional financial services and products, although there needs to be ongoing monitoring for any potential changes. Most detected cases involved the use of one type of virtual asset only. In cases where criminals did make use of more than one type of virtual asset, such use was primarily for the layering of illicit proceeds. While cases provided by jurisdictions typically focused on ML or on predicate offences, criminals did make use of virtual assets to evade financial sanctions and to raise funds to support terrorism. Overall, the use of virtual assets as a way of layering is the most prominent typology observed in the cases, possibly due to the ease of rapid transfer (e.g. updating public addresses and fast exchanges across borders). Professional ML networks have also appeared to start exploiting this vulnerability and use virtual assets as one of their means to launder illicit proceeds.

17. The types of offences involving virtual assets include ML, the sale of controlled substances and other illegal items (including firearms), fraud, tax evasion, sanctions evasion, computer crimes (e.g. cyberattacks resulting in thefts), child exploitation, human trafficking and TF. Among them, narcotics-related and fraud offences (e.g. investment scams and swindling, blackmail, and extortion) are the most prevalent. Jurisdictions which have incorporated virtual assets and VASPs in their domestic AML/CFT regime also noted offences related to operating unlicensed or unauthorised financial services, record keeping, and reporting requirements.

18. The main trends in the virtual asset ML/TF risk landscape since June 2019 include:

- a) the use of VASPs registered or operating in jurisdictions that lack effective AML/CFT regulation, as well as the use of multiple VASPs (local and/or overseas). This makes it more challenging for competent authorities to follow the transaction trail, buying more time for criminals to move criminal proceeds.
- b) the continued use of tools and methods to increase the anonymity of transactions. This includes registering Internet domain names through proxies and using DNS registrars that suppress or redact the true owners of the domain names, the use of tumblers, mixers and anonymity-enhanced cryptocurrencies or privacy coins, using decentralised exchanges and applications, chain-hopping and atomic swapping exchanges (which allow the exchange of one type of virtual asset to another without going through an exchange) and dusting (which allows the transfer of tiny amounts of virtual assets to random wallets, making it more difficult to track and trace the transaction trail).

19. In response to the ongoing COVID-19 pandemic, FATF jurisdictions have also observed the increased use of virtual assets to move and conceal illicit funds. One jurisdiction reported the use of virtual assets to launder proceeds earned from selling COVID-19 medicine.⁵

Trends in virtual asset market structure

20. Looking more broadly at the virtual asset market since June 2019, global government attention has largely focused on proposed so-called “stablecoins” with potential for mass-adoption. So-called stablecoins are a type of asset that purport to maintain a stable price relative to reference assets. The proposed launch of these arrangements has brought significant attention to whether their mass-adoption would lead to a substantial increase in the number of anonymous peer-to-peer virtual asset transactions occurring via unhosted wallets. Peer-to-peer transactions, without the use of a VASP or other AML/CFT-regulated entity, are not explicitly covered by the revised FATF Standards.

21. A rapid expansion in the number and value of transactions not subject to AML/CFT controls under the revised FATF Standards would however present a material ML/TF vulnerability. Therefore, jurisdictions should assess and determine the ML/TF risks they face with virtual assets. The ML/TF risks of virtual assets are more difficult to address and mitigate once the products are launched. Their cross-border nature can present difficulties for enforcement if AML/CFT is not considered from the start. Hence, it is very important for jurisdictions to analyse and address risk in a forward-looking manner and ensure that they have all the necessary tools and authorities in place before they are needed.

22. The FATF’s views on so-called stablecoins are set out in its report to the G20 and are considered further in Section 4 below.⁶

⁵ FATF, [Covid-19-related Money Laundering and Terrorist Financing: Risks and Policy Response](#), May 2020

⁶ FATF, [Report to G20 on so-called stablecoins](#), June 2020

Section 2: State of implementation by the public sector

23. This section sets out jurisdictions' state of implementation of the revised FATF Standards on virtual assets and VASPs. This overview is based on the survey the FATF conducted in March 2020 of its membership and its broader Global Network. Thirty-eight FATF members (37 jurisdictions and 1 regional organisation) and 16 FSRB member jurisdictions responded. The questionnaire was a self-assessment by participating jurisdictions and is not an official FATF assessment of the level of implementation of jurisdictions.

24. The results of the questionnaire indicate that, overall, jurisdictions have made progress in implementing the revised FATF Standards (R.15/INR.15). Under the revised FATF Standards, jurisdictions may either permit and regulate VASPs or prohibit them and enforce the prohibition. Twenty-four FATF members and eight FSRB members, advised that they had introduced a regulatory regime permitting VASPs (Table 1). One FATF member and two FSRB members advised that they had prohibited VASPs.

25. Nonetheless, 19 jurisdictions, comprising 13 FATF members and 6 FSRB members, reported that they do not have a regime for VASPs yet. This gap is potentially much larger across the FATF's broader Global Network. Again, the majority of these (13) intended to regulate VASPs, two intended to prohibit VASPs and four had yet to decide. For those who had not yet implemented an AML/CFT regime for VASPs, there was a wide variation in what stage of the process they were at. At least eight of these jurisdictions reported that they were in the process of passing the necessary legislation or consulting on the design of their regime.

26. For those jurisdictions that regulate VASPs, the majority advised that they have introduced new legislation to specifically regulate VASPs. Most jurisdictions appear to have done this by adding VASPs as an obliged entity to their existing law. Several jurisdictions considered that VASPs were covered by their existing AML/CFT laws. There is a wide range of terms used to refer to VASPs, with at least eleven different terms reported (e.g., VASP, digital asset business, cryptoasset exchange provider). There does not seem to be an emerging common terminology for virtual assets and VASPs in terms of jurisdictions' legislative definitions.

Table 1. Progress in implementing VASP AML/CFT regulatory regimes

	FATF	FSRB	Total
Regulation of VASPs			
AML/CFT regime permitting VASPs is established	24	8	32
Regulations being developed / approved to regulate VASPs	9	4	13
Prohibition of VASPs			
VASPs prohibited with prohibition enforced	1	2	3
Regulations being developed / approved to prohibit VASPs	2	0	2
Yet to decide			
Approach to VASPs under consideration	2	2	4
TOTAL	38	16	54

27. For the 32 jurisdictions which advised that they have established regimes permitting VASPs, 30 have introduced either registration (18 jurisdictions) or

licencing regimes (14 jurisdictions).⁷ All advised that they have included minimum option of VASPs created in their jurisdiction as required by the revised FATF Standards. Eighteen jurisdictions advised that they have extended their regime to include VASPs incorporated overseas but which offer products/services to customers in their jurisdiction and 20 jurisdictions advised that they have extended their regime to include VASPs conducting operations from their jurisdiction. This diversity in approach may present challenges in identifying which VASPs are regulated by each jurisdiction. Nineteen jurisdictions reported that they had publicly available list(s) of VASPs that they have registered or licenced.

28. Twenty-three of these jurisdictions advised that they have begun licencing / registering VASPs. The 20 jurisdictions which provided data reported that they have 1 133 registered or licenced VASPs across them. Most jurisdictions reported less than ten registered or licenced VASPs, although four reported 100 or more VASPs. Several jurisdictions noted challenges in identifying the VASPs for registration or licencing under their AML/CFT regimes.

29. For the jurisdictions that have implemented regulatory regimes permitting VASPs, they reported that they had implemented the full range of preventive measures required under the FATF Standards (Recommendations 10-21 as set out in INR.15). The exception is implementation of the ‘travel rule’ (see Section 4). Regarding suspicious transaction reporting, 19 jurisdictions provided STR data on reports from VASPs. These 19 jurisdictions reported 134 500 STRs reported by VASPs between 2018 and March 2020. Most jurisdictions reported financial institutions, in particular banks and payment service providers, as being the main reporters of STRs about virtual assets. It is difficult to draw any other distinct trends from jurisdictions’ reporting, as there is wide variation between different jurisdictions’ numbers.

30. Of the 32 jurisdictions which reported that they have a regulatory regime for VASPs, 31 of these have a supervisory regime.⁸ A range of different organisations have been designated as VASP supervisors, including financial services supervisors, central banks, securities regulators, tax authority and specialist VASP supervisors, and some jurisdictions have multiple supervisors. Twenty-eight of these jurisdictions advised that they have allocated supervisory staff for VASP supervision and 25 reported that they were undertaking a risk-based approach to supervision of VASPs. Fifteen jurisdictions reported that they have already conducted on- and/or off-site inspections of VASPs and eight reported that they had imposed criminal, civil and/or administrative sanctions on VASPs for non-compliance with AML/CFT obligations. This includes the cancellation, refusal or suspension of VASPs’ registrations, administrative sanctions to improve VASP compliance, public warnings, civil monetary penalties and criminal sanctions.

31. Supervisors advised that they are using a wide range of information to inform their risk-based approach, including information collected through the registration or licencing process, compliance information, reporting from VASPs, information from supervisory activities and partner agencies and open source information. Several jurisdictions noted that they were using, or planning to use, ‘SupTech’ tools, such as blockchain analysis software. Jurisdictions also generally noted the challenges faced

⁷ Two jurisdictions have both a licencing and registration regime for different kinds of VASPs.

⁸ One FATF member (a regional organisation) does not directly supervise entities for compliance with AML/CFT regulations.

in supervising the VASP sector, where regulation is generally nascent and where VASPs generally have little experience or expertise in AML/CFT.

32. Jurisdictions noted a range of outreach activities to the VASP sector, including the dissemination of the results of risk assessments, risk indicators, red flags, advisories, typologies, guidance, training, industry consultation and events, public-private partnerships and annual reports and analysis of the VASP sector.

33. Thirty-four jurisdictions reported that they had assessed the ML/TF risks posed by virtual assets and VASPs. To conduct the risk assessments posed by virtual assets and VASPs, some jurisdictions reported they conducted such assessments through multi-agency groups. Regarding information they use for risk assessments, there are different information sources depending on jurisdictions, including FIU information (including STRs), law enforcement cases involving virtual assets, VASPs supervisory information, international co-operation requests, transactions involving virtual assets and internet information on activity of virtual assets and VASPs.

34. In terms of international co-operation, jurisdictions noted the presence of pre-existing memoranda of understanding and international co-operation frameworks that could enable co-operation in the supervision of VASPs. The FATF has a project underway to improve international co-operation amongst VASP supervisors, particularly relating to information-sharing and capability building amongst supervisors.

35. For the five jurisdictions that reported that they prohibit, or plan to prohibit VASPs, a range of tools and techniques were highlighted as ways to enforce the prohibition. This included the use of risk assessments, public information campaigns, supervisory activity and STRs from financial institutions to identify illicit virtual asset activity and the development of bespoke technological tools in order to identify illicit virtual asset activity.

36. A range of practical challenges have also been identified in implementing the revised FATF Standards where jurisdictions have requested greater Guidance. These areas are elaborated in Section 4.

Section 3: State of implementation by the private sector

37. This section sets out the state of implementation of the revised FATF Standards on virtual assets and VASPs by the VASP sector. It is based on information collected through the FATF questionnaire, the Virtual Assets Contact Group's outreach to a selection of representatives from the VASP sector and travel rule technology providers in February and April 2020 and the outcomes from the Financial Services Agency of Japan's March 2020 roundtable on the travel rule. The FATF intended to engage the broader VASP sector through its annual Private Sector Consultative Forum in May 2020, however this was delayed due to the COVID-19 pandemic. The meetings with the Contact Group only encompassed a selection of VASP representatives and technology providers, so the information collected, and the results outlined in this report, cannot be taken to represent the entirety of the global VASP sector.

Implementation of the travel rule

38. VASPs are required to implement the FATF's AML/CFT preventive measures in Recommendations 10-21 as set out in INR.15. This includes Recommendation 16 (R.16), which sets out wire transfer requirements. It is a key AML/CFT measure to ensure that originators and beneficiaries of financial transactions are identifiable and are not anonymous. VASPs and financial institutions must comply with these requirements for virtual asset transfers.⁹ This is the so-called 'travel rule' and is the issue of most focus in terms of VASPs' compliance with the revised FATF Standards.

39. There are various technologies and tools available that could enable VASPs to comply with aspects of the travel rule requirements. While the FATF is technology-neutral and does not prescribe a particular technology or software, the FATF Guidance on virtual assets and VASPs published in June 2019 lists a range of technologies which may enable VASPs to comply with aspects of the travel rule requirements.¹⁰ These tools existed when the FATF Standards were revised in June 2019. There was not, however, technological solution(s) that enabled VASPs to comply with all aspects of the travel rule in a holistic, instantaneous and secure manner.

40. The FATF has been monitoring the progress by the VASP sector in developing these solutions and complying with R.16 requirements. Based on the outreach through the Virtual Assets Contact Group with a selection of representatives of the VASP sector and travel rule technology providers, there seems to have been progress in developing technological solutions for the travel rule.

41. Firstly, there has been progress in the development of technological standards for use by different travel rule solutions. The FATF is aware of an international industry-wide initiative that has been established to set global technical standards for travel rule solutions to use. They have developed a first messaging standard which sets a common universal language for the communication of the required originator and beneficiary information between VASPs. The FATF is aware that this initiative

⁹ See Annex A for the full requirements.

¹⁰ These include public and private keys, Transport Layer Security/Secure Sockets Layer connections, X.509 certificates, X.509 attribute certificates and API technology.

may now be undertaking work on further messaging standards and the maintenance of this standard.

42. In addition, several different travel rule technology solutions are being developed, with some solutions being launched or being tested. Some of these solutions are being developed by VASPs to be integrated into their systems. Others are technology solutions that could be used by multiple VASPs. In line with decentralisation ethos that underpins virtual assets, there appears to be a general desire for multiple potential solutions, rather than one centralised travel rule solution. The usage of common standards will assist in ensuring different solutions are interoperable. Nonetheless, the FATF is not aware yet that there are sufficient holistic technological solutions for global travel rule implementation that have been established and widely adopted.

43. In terms of jurisdiction implementation, there has been less implementation of travel rule requirements for VASPs than other AML/CFT requirements. From the 32 jurisdictions that have implemented AML/CFT regulatory requirements for VASPs, 15 jurisdictions advised they had introduced R.16 requirements for VASPs. Some jurisdictions noted they were enforcing R.16 requirements, but several others stated that they had faced difficulty enforcing the R.16 requirements effectively and had delayed enforcement while waiting for holistic and scalable technological solutions to be developed. Seventeen jurisdictions advised that they had not introduced R.16 requirements for VASPs, with the delay generally again attributed to the lack of adequate holistic technology solutions. Those jurisdictions who had not introduced R.16 requirements advised that they were engaging with the VASP sector to promote the development of technological solutions and identify the issues and challenges to be addressed, including through outreach of the Contact Group.

44. This delay in introducing R.16 requirements for VASPs adds to the importance of the quick development of technology solutions. Several jurisdictions noted that the travel rule represented a significant challenge to the effective implementation of the revised FATF Standards. As set out in Section 4, this review has also identified a range of issues which impact the implementation of the travel rule, which should be addressed so that there can be the effective implementation of R.16 requirements by jurisdictions in an efficient, sector-wide manner.

45. This review, however, does not consider that these are fundamental barriers to the continued development of technological solutions to implement the travel rule. As jurisdictions should fully implement AML/CFT obligations for VASPs, including the travel rule, the FATF calls upon the VASP sector to redouble its efforts towards the swift development of holistic technological solutions encompassing all aspects of the travel rule. Further outreach and engagement by the FATF with a diversified selection of VASPs should help to address these issues, develop a more comprehensive view of the remaining challenges and encourage the development of technology solutions or other means of effective compliance with the travel rule. Further clarification by FATF and national authorities on the issues identified in Section 4 and coordinated actions by national authorities should also assist.

Implementation of other AML/CFT obligations

46. Implementation of other AML/CFT obligations globally appears to be at early stages. As a relatively new sector, VASPs may not have a history of regulatory oversight and may be unfamiliar with the fundamentals of AML/CFT. This challenge

is further complicated by the rapid technological and business progress in the VASP sector, where there is a constant evolution in technology, services, business practices and firms entering and exiting the market.

47. Nonetheless, some jurisdictions have more developed AML/CFT regimes for VASPs and have imposed obligations on VASPs for a longer period of time. They reported improvements in overall compliance, with increasing awareness and attention to AML/CFT obligations, particularly among larger, established VASPs. The most common citations noted for VASPs arising from examinations included deficiencies related to internal control, independent testing, and record-keeping. These deficiencies can be related to common issues VASPs may exhibit, such as expanding operations more rapidly than their compliance function can manage, failing to implement adequate controls to mitigate risks involved with anonymity-enhanced virtual assets, reliance on manual transaction testing and not conducting appropriate levels of due diligence to understand the risk profile of customers' activity off-platform.

Section 4: Issues identified with the revised FATF Standards and Guidance

48. Jurisdictions and representatives from the VASP sector have identified a range of issues regarding the implementation of the revised FATF Standards and Guidance on virtual assets and VASPs. These issues were identified through the FATF questionnaire and the Virtual Assets Contact Group's outreach to a selection of representatives from the VASP sector.

49. The information provided does not identify any issue that requires the revised Standards to be amended at this point in time. There are numerous issues however where jurisdictions and VASPs have asked for greater and clearer FATF Guidance and sustained outreach and collaboration. This could include tailored guidance for low-capacity countries.

Definition of virtual asset and VASP

50. The amendments to the FATF Standards introduced the new terms 'virtual asset' and 'virtual asset service provider' (see **Annex A**). As jurisdictions have transposed the revised FATF Standards into their national laws, they have noted areas where there could be greater clarity in the FATF Guidance. Regarding the definition of virtual assets, there could be greater clarity about what approach jurisdictions should take if a new asset is developed that could be categorised as a traditional financial asset under the revised FATF Standards but is based on the technology associated with virtual assets. For example, this issue has particularly arisen in the context of so-called stablecoins and whether jurisdictions should be treating them as traditional financial assets / financial institutions or virtual assets / VASPs if these are regulated under two separate AML/CFT regimes.

51. Jurisdictions also saw a need for greater FATF Guidance on the scope of the activities covered by the definition of VASP. In particular, jurisdictions considered that there could be greater clarity regarding the scope of the activities of 'safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets', 'participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset' and the activities covered by 'transfer of virtual assets' that are not covered by the other limbs of the definition. Ensuring consistency in the definition of VASP is important to ensure that there is a common standard applied regarding which businesses are covered as VASPs in jurisdictions. As the FATF and its Global Network conduct more mutual evaluations and follow-up reports of members, the extent to which jurisdictions are fully implementing the FATF definition of VASP will also become clearer.

Peer-to-peer transactions and private / non-custodial wallets

52. Currently, peer-to-peer transfers of virtual assets, without the use or involvement of a VASP or financial institution, are not explicitly subject to AML/CFT obligations under the revised FATF Standards. The lack of explicit coverage of peer-to-peer virtual asset transactions of this type was deliberate, as the revised FATF Standards' general focus is on placing AML/CFT obligations on intermediaries between individuals and the financial system. The lack of explicit coverage of peer-to-peer transactions via private / unhosted wallets was a source of concern for a number

of jurisdictions. Jurisdictions noted that transfers to the unregulated peer-to-peer sector could present a leak in tracing illicit flows of virtual assets.

53. However, jurisdictions did not consider that there was sufficient evidence to warrant changing the revised FATF Standards at this point in time. There was insufficient evidence demonstrating that the number and value of anonymous peer-to-peer transactions has changed enough since June 2019 to present a materially different ML/TF risk. Further research could be undertaken with the VASP sector, academics and software experts and engineers to better understand the scope of the unregulated peer-to-peer sector.

54. The launch of new virtual assets however could materially change the ML/TF risks, particularly if there is mass-adoption of a virtual asset that enables anonymous peer-to-peer transactions. There are a range of tools that are available at a national level to mitigate, to some extent, the risks posed by anonymous peer-to-peer transactions if national authorities consider the ML/TF risk to be unacceptably high. This includes banning or denying licensing of platforms if they allow unhosted wallet transfers, introducing transactional or volume limits on peer-to-peer transactions or mandating that transactions occur with the use of a VASP or financial institutions. As of yet, no common practices or consistent international approach have emerged regarding the use of these different tools. Accordingly, there should be further work undertaken on the extent to which anonymous peer-to-peer transactions via unhosted wallets is occurring, the approach jurisdictions can take to mitigate the ML/TF risks, the extent to which the revised Standards enable jurisdictions to mitigate these risks and to continue to improve international co-operation and co-ordination.

So-called stablecoins

55. A key development since the finalisation of the revisions to the FATF Standards has been the emergence of proposals for so-called stablecoins. Some proposals for so-called stablecoins have the potential to be mass-adopted on a scale not seen in pre-existing virtual assets. Depending on their design and national laws, they may be a virtual asset or traditional financial asset under the revised FATF Standards.

56. As set out in the FATF's report to the G20, the revised FATF Standards apply to so-called stablecoins and their providers either as financial institutions or VASPs.¹¹ Based on known models, the FATF considered that the current revised FATF Standards are sufficient to mitigate the ML/TF risks posed by so-called stablecoins at this point in time, if jurisdictions have fully implemented the revised FATF Standards.

57. Nonetheless, the FATF identified that this area must be closely monitored, as there are residual risks relating to anonymous peer-to-peer transactions via unhosted wallets, jurisdictions with weak or non-existent AML/CFT regulation and so-called stablecoins with decentralised governance. In addition, so-called stablecoins raise a range of practical challenges for jurisdictions where updated FATF Guidance would assist, including the tools, powers, skills and expertise supervisors may need to effectively regulate so-called stablecoins and situations where jurisdictions may wish to prohibit a specific so-called stablecoin proposal.

¹¹ FATF, [Report to G20 on so-called stablecoins](#), June 2020

Identifying VASPs for registration / licencing

58. Jurisdictions have taken different approaches as to which VASPs they have covered in their AML/CFT regimes. Under the revised FATF Standards, jurisdictions must regulate VASPs created in their jurisdiction, but can chose to expand their coverage to VASPs offering services to their citizens or with operations in their jurisdiction.

59. A number of jurisdictions noted challenges in identifying the VASPs they should cover under their AML/CFT regimes. In particular, several queried what approach they should take regarding VASPs offering products and/or services to customers in their jurisdiction, but are domiciled elsewhere or have no physical presence in their jurisdiction. Jurisdictions also raised the best way to identify the appropriate 'home' supervisor(s) for VASPs, particularly if a VASP is decentralised and has no obvious 'home' jurisdiction in which it is based. These jurisdictions asked for further guidance on how to identify VASPs for registration / licencing and the responsibilities of different supervisors where a VASP is decentralised. This underscores the importance of effective international co-operation and the development of standard protocols of co-operation between VASP supervisors. It is also a challenge shared by the private sector, as set out below.

Travel rule implementation

60. A range of identified issues remain which impact the full, effective and smooth implementation of a global framework for the travel rule. These are discussed below and point generally to a need for further FATF Guidance and engagement on the travel rule. There is a strong desire from representatives from the VASP sector for continued engagement with the FATF and members as travel rule solutions develop and mature.

61. **Identifying counterparty VASPs.** In order to comply with the travel rule, VASPs must be able to identify when they are (a) transacting with another VASP (as opposed to a private wallet) and (b) whether the counterparty VASP is registered / licenced by a jurisdiction and adequately supervised for AML/CFT purposes. The best way to conduct counterparty due diligence in a timely and secure manner is a challenge.

62. One way to address this issue which has been raised by the private sector is the creation of a 'global list of VASPs'. In this approach, information on licensed and registered VASPs would be collected from each jurisdiction's list and accessed through a central database (in a centralised approach) or accessed through an API / smart contracts which connect to each jurisdiction's list (in a decentralised approach). Creation of a global list of VASPs raises a number of challenges, including how to ensure the accuracy and security of the information, who is responsible for collecting and maintaining the information (governance), who would supervise the bod(ies) responsible for collecting their information and who would have access to this information in light of potential derisking risks relating to the publication of a list of VASPs. All of these would need to be addressed before a robust solution could be developed. Further, there may be other options available to assist VASPs in identifying their counterparties.

63. **Peer-to-peer transactions via private / unhosted wallets.** Peer-to-peer transfers of virtual assets, without the use or involvement of a VASP or financial institution, are not explicitly subject to AML/CFT obligations under the revised FATF

Standards. Several VASPs have queried about what approach should be taken to their transacting with private or unhosted wallets. There is an initial issue about the extent to which a wallet can be identified as a custodial vs a non-custodial wallet. This has led some VASPs to ask for Guidance on the extent to which blockchain analytic tools can be used in complying with travel rule requirements. A second issue is then whether VASPs should be able to transact with private wallets and, if so, what kind of AML/CFT requirements need to be put in place to mitigate the risks. It should be noted that VASPs' best practice and procedures to meet AML/CFT obligations (e.g. sanctions screening) could be different from those of banks and other traditional financial institutions, given the nature of blockchain, and further clarification by FATF or national authorities could also help VASPs to meet AML/CFT obligations in a coordinated and effective manner. Some VASPs have also raised the risk that unnecessarily burdensome AML/CFT compliance obligations, including the travel rule, may incentivise greater use of peer-to-peer transactions via unhosted wallets, raising the risks and requiring further mitigation measures.

64. **Batch and post facto submission and past transfers.** Some VASPs have requested guidance on the extent to which the batched data submission of transfers of originator and beneficiary data is permissible under the revised FATF Standards. They have queried whether originator and beneficiary data could be submitted on the post facto basis (e.g. at the end of the day, or five to six business days later), instead of the immediate data submission on an individual virtual asset transfers. Some VASPs have also requested further Guidance on the extent to which beneficiary and originator data should be collected on past virtual asset transfers.

65. **Inter-operability of systems.** For implementation of the travel rule to progress smoothly globally, different solutions need to be inter-operable, with adequate controls in place to address data sharing, storage and security. This will reduce compliance costs for VASPs and limit the fragmentation of VASP markets into different systems. The development of global messaging standards is a first step in ensuring that systems can be interoperable. However, fragmentation may be driven by factors such as different rules for privacy and data protection, cyber-security or AML/CFT, such as where one jurisdiction requires "purpose of transaction" as mandatory information when another does not. Different rules and standards in different jurisdictions may impact the inter-operability of different travel rule solutions, unless sufficient flexibility is built into the messaging standards/solutions being developed to accommodate the requirements of particular jurisdictions. This highlights the importance of close co-operation with and within the private sector and amongst jurisdictions in developing their AML/CFT regimes and supervisory approaches.

66. **Sunrise issue.** At this point in time, less than half of FATF members have introduced travel rule requirements for VASPs and this gap may be larger in the FATF's broader Global Network. This means there is not yet a global framework for travel rule compliance. VASPs have raised this as a challenge as it means it is unclear what approach they should take in dealing with VASPs located in jurisdictions without the travel rule (the 'sunrise issue'). This issue will remain until all jurisdictions have introduced the requirement.

67. Some VASPs have asked for greater guidance from the FATF and supervisors on the approach they should take, particularly whether they can transact with VASPs in jurisdictions without travel rule requirements and, if so, what data can and should

be securely transmitted. Some VASPs have proposed that FATF expressly state that jurisdictions can provide an exemption for transmitting data only for such time as receiving VASPs are not licensed/registered and/or an operational travel rule system is not in place.

68. **Specific wording issues.** Several specific wording issues with the FATF Guidance regarding R.16 for VASPs were raised, including references to the Legal Entity Identifier, the term 'account number' and the address of an originator.

Section 5: Proposed next steps

69. Overall, many jurisdictions and the VASP sector have made progress in implementing the revised FATF Standards on virtual assets and VASPs. Over half the FATF membership reported that they have now incorporated the revised FATF Standards into their domestic law and there now appear to be the first technology solutions for the travel rule appearing on the market. However, challenges remain. Some jurisdictions' AML/CFT regime for VASPs are not yet operational and some have not yet established regimes. This review has not surveyed the entirety of the FATF Global Network, so the level of progress amongst non-reporting FSRB members is unknown.

70. At this stage in time, there is no clear need to amend R.15/INR.15. While there are many areas where both jurisdictions and the private sector seek further clarity, updated FATF Guidance should be pursued in the first instance. The FATF should consider future amendments to the revised Standards if this work identifies issues which updated Guidance cannot resolve. The FATF must also closely monitor the risks posed by so-called stablecoins, anonymous peer-to-peer transactions via unhosted wallets and the broader virtual asset market. If there does appear to be a significant change to the market structure or ML/TF risk profile, the FATF should consider whether amendments to the revised Standards are warranted.

71. As public and private sector implementation of the revised Standards is still ongoing, and most jurisdictions' AML/CFT regimes for VASPs are nascent, this review proposes that FATF should continue to actively monitor and support implementation of the new requirements by jurisdictions. The FATF should also continue its engagement with the VASP sector and technology providers. The FATF will also work collaboratively with other global standard-setting bodies to ensure a coordinated approach to virtual assets.

72. Therefore, this review recommends the FATF undertake the following actions focused on virtual assets and VASPs:

- a) **The FATF need not amend its revised Standards on virtual assets and VASPs at this point in time, but should conduct a second 12-month review of the implementation of the revised FATF standards by June 2021 and consider whether further updates are necessary.** As the virtual asset market evolves quickly, the FATF considers that the virtual assets and VASP sector continues to warrant enhanced monitoring. A second 12-month review would provide a longer timeframe to observe changes to the virtual asset market and the impact of the revised FATF Standards. By June 2021, jurisdictions will have had two years to transpose the revised FATF Standards on VASPs into law and the VASP sector will have had time to implement travel rule solutions globally. The FATF and its Global Network will also have completed more mutual evaluation and follow-up reports, which will assess jurisdictions' compliance with the revised FATF Standards and identify any other possible challenges in implementing the Standards. The work will cover progress by the public and private sectors, consider issues such as travel rule implementation and anonymous peer-to-peer virtual asset transactions via unhosted wallets and seek to collect better market metrics on virtual assets, especially on the volume and proportion of peer-to-peer virtual asset transactions.

- b) **The FATF should release updated Guidance for the public and private sectors.** This updated Guidance should address the issues outlined in this report, particularly the issues identified in Section 4, including so-called stablecoins and travel rule implementation.
- c) **The FATF should continue to promote the understanding of the public and national authorities of the ML/TF risks involved in transactions using virtual assets and the potential misuse of virtual assets for ML/TF purposes.** To this end, the FATF will make available information on red flag indicators associated with virtual assets transactions to the public in October 2020.
- d) **The Virtual Asset Contact Group should continue and enhance its engagement with the private sector.** The Contact Group has been a useful forum for progressing the FATF's work on virtual assets. In February 2020, it began directly liaising with a selection of VASP representatives. This has been valuable in enabling the FATF to monitor progress on travel rule implementation and build relationships with the VASP sector. These VASPs representatives have greatly appreciated this outreach and have asked for an enhanced dialogue between the FATF and the sector. This engagement should continue, particularly focusing on monitoring progress on implementation of the travel rule. The FATF should seek to engage with the broader VASP community, as well as technical experts and academics, through the FATF's Private Sector Consultative Forum and other relevant forums.
- e) **The FATF should continue its program of work to enhance international co-operation amongst VASP supervisors.** An effective global response to virtual assets requires effective co-operation amongst supervisors. The FATF's Policy Development Group will consider proposals on how to enhance international co-operation amongst VASP supervisors in October 2020 and a third meeting of the VASP Supervisors' Forum will occur by November 2020.

Annex A. Recommendation 15 and its Interpretive Note and FATF Definitions

Recommendation 15 – New Technologies

73. Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

74. To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.

Interpretative Note to Recommendation 15

75. For the purposes of applying the FATF Recommendations, countries should consider virtual assets as “property,” “proceeds,” “funds,” “funds or other assets,” or other “corresponding value.” Countries should apply the relevant measures under the FATF Recommendations to virtual assets and virtual asset service providers (VASPs).

76. In accordance with Recommendation 1, countries should identify, assess, and understand the money laundering and terrorist financing risks emerging from virtual asset activities and the activities or operations of VASPs. Based on that assessment, countries should apply a risk-based approach to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. Countries should require VASPs to identify, assess, and take effective action to mitigate their money laundering and terrorist financing risks.

77. VASPs should be required to be licensed or registered. At a minimum, VASPs should be required to be licensed or registered in the jurisdiction(s) where they are created.¹² In cases where the VASP is a natural person, they should be required to be licensed or registered in the jurisdiction where their place of business is located. Jurisdictions may also require VASPs that offer products and/or services to customers in, or conduct operations from, their jurisdiction to be licensed or registered in this jurisdiction. Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a VASP. Countries should take action to identify natural or legal persons that carry out VASP activities without the requisite license or registration, and apply appropriate sanctions.

¹² References to creating a legal person include incorporation of companies or any other mechanism that is used.

78. A country need not impose a separate licensing or registration system with respect to natural or legal persons already licensed or registered as financial institutions (as defined by the FATF Recommendations) within that country, which, under such license or registration, are permitted to perform VASP activities and which are already subject to the full range of applicable obligations under the FATF Recommendations.

79. Countries should ensure that VASPs are subject to adequate regulation and supervision or monitoring for AML/CFT and are effectively implementing the relevant FATF Recommendations, to mitigate money laundering and terrorist financing risks emerging from virtual assets. VASPs should be subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements. VASPs should be supervised or monitored by a competent authority (not a SRB), which should conduct risk-based supervision or monitoring. Supervisors should have adequate powers to supervise or monitor and ensure compliance by VASPs with requirements to combat money laundering and terrorist financing including the authority to conduct inspections, compel the production of information, and impose sanctions. Supervisors should have powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the VASP's license or registration, where applicable.

80. Countries should ensure that there is a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with VASPs that fail to comply with AML/CFT requirements, in line with Recommendation 35. Sanctions should be applicable not only to VASPs, but also to their directors and senior management.

81. With respect to preventive measures, the requirements set out in Recommendations 10 to 21 apply to VASPs, subject to the following qualifications:

- a) R.10 – The occasional transactions designated threshold above which VASPs are required to conduct customer due diligence is USD/EUR 1 000.
- b) R.16 – Countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information¹³ on virtual asset transfers, submit¹⁴ the above information to the beneficiary VASP or financial institution (if any) immediately and securely, and make it available on request to appropriate authorities. Countries should ensure that beneficiary VASPs obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers, and make it available on request to appropriate authorities. Other requirements of R.16 (including monitoring of the availability of information, and taking freezing action and prohibiting transactions with designated persons and entities) apply on the same basis as set out in R.16. The same obligations apply to financial institutions when sending or receiving virtual asset transfers on behalf of a customer.

82. Countries should rapidly, constructively, and effectively provide the widest possible range of international co-operation in relation to money laundering, predicate offences, and terrorist financing relating to virtual assets, on the basis set

¹³ As defined in INR. 16, paragraph 6, or the equivalent information in a virtual asset context.

¹⁴ The information can be submitted either directly or indirectly. It is not necessary for this information to be attached directly to virtual asset transfers.

out in Recommendations 37 to 40. In particular, supervisors of VASPs should exchange information promptly and constructively with their foreign counterparts, regardless of the supervisors' nature or status and differences in the nomenclature or status of VASPs.

FATF Glossary

A **virtual asset** is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.

Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- i. exchange between virtual assets and fiat currencies;
- ii. exchange between one or more forms of virtual assets;
- iii. transfer¹⁵ of virtual assets;
- iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
- v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

¹⁵ In this context of virtual assets, transfer means to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another.

References

FATF, [*Covid-19-related Money Laundering and Terrorist Financing: Risks and Policy Response*](#), May 2020.

FATF, [*Report to G20 on so-called stablecoins*](#), June 2020

FATF, [*Switzerland: 2nd Enhanced Enhanced Follow-up Report and Technical Compliance Re-Rating*](#), January 2020

FATF, [*United States: 2nd Enhanced Follow-up Report and Technical Compliance Re-Rating*](#), March 2020

The FATF logo is a red, rounded rectangular shape with a white stylized graphic of a person's head and shoulders inside. The letters "FATF" are written in white, bold, sans-serif font at the top of the red shape.

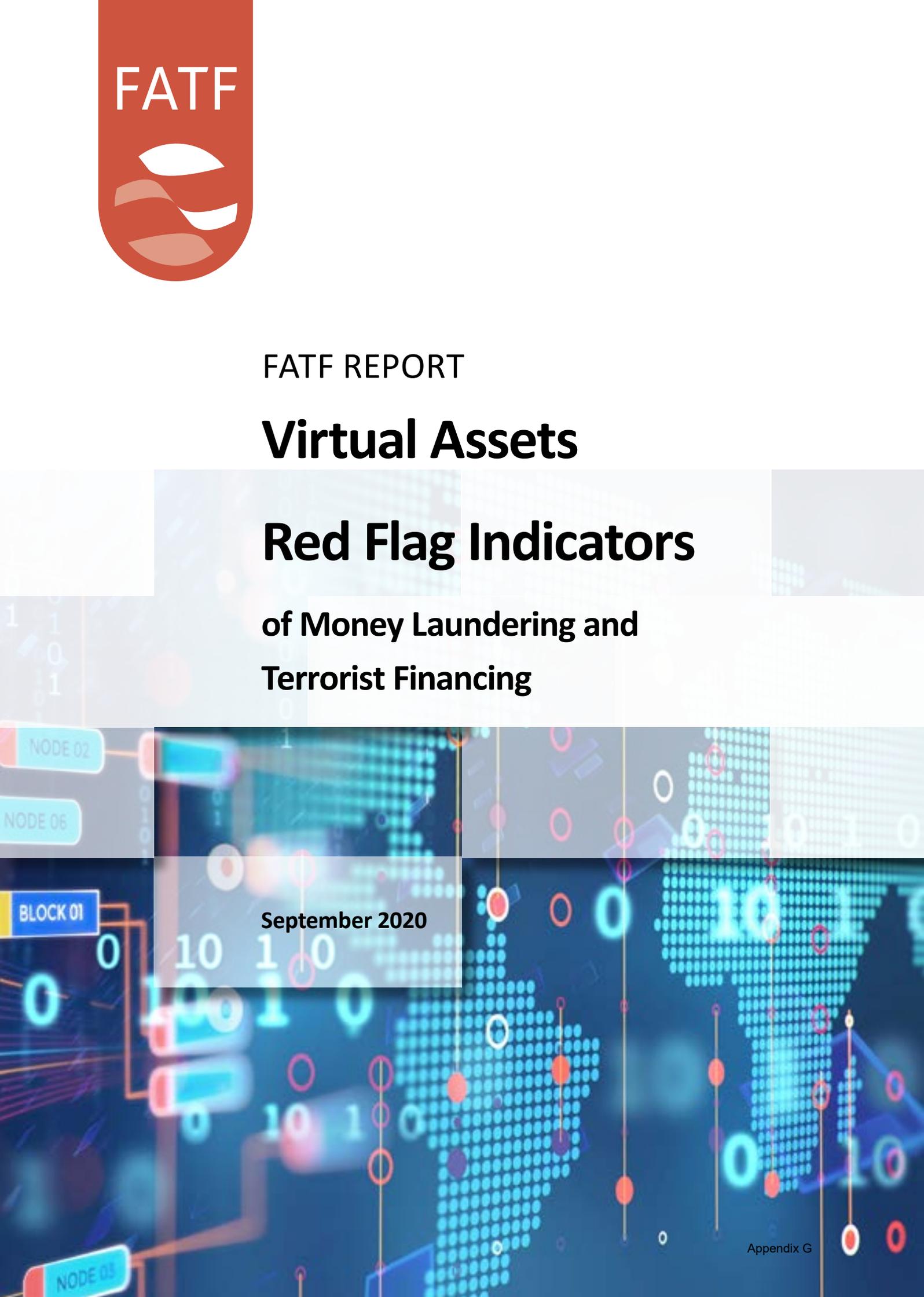
FATF

FATF REPORT

Virtual Assets

Red Flag Indicators

of Money Laundering and
Terrorist Financing

The background of the cover is a complex digital graphic. It features a dark blue and black color palette with glowing cyan and red elements. There are binary digits (0s and 1s) scattered throughout, some in a grid pattern. On the left side, there are several rectangular nodes labeled "NODE 01", "NODE 02", "NODE 03", and "NODE 06", connected by lines. A central area contains a glowing globe or map of the world, composed of a grid of small dots. The overall aesthetic is futuristic and technological.

September 2020



The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit www.fatf-gafi.org

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2020), *Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets*, FATF, Paris, France,
www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html

© 2020 FATF/OECD. All rights reserved.

No reproduction or translation of this publication may be made without prior written permission.

Applications for such permission, for all or part of this publication, should be made to the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France (fax: +33 1 44 30 61 37 or e-mail: contact@fatf-gafi.org)

Photocredits coverphoto ©Gettyimages

Table of Contents

Acronyms	2
Introduction	3
Methodology and sources used in drawing up the list of red flag indicators	4
Issues to note when reading this Report	4
Red Flag Indicators	5
Red Flag Indicators Related to Transactions	5
Red Flag Indicators Related to Transaction Patterns	7
Red Flag Indicators Related to Anonymity	9
Red Flag Indicators about Senders or Recipients	12
Red Flag Indicators in the Source of Funds or Wealth	15
Red Flag Indicators Related to Geographical Risks	17
Conclusion	19
References	20

Acronyms

AEC	Anonymity enhanced cryptocurrency
CDD	Customer due diligence
DNFBPs	Designated non-financial businesses and professions
DNS	Domain name registrars
FATF	Financial Action Task Force
FIs	Financial Institutions
FIUs	Financial Intelligence Units
ICO	Initial Coin Offering
KYC	Know-your-customer
LEAs	Law enforcement authorities
ML	Money Laundering
STRs	Suspicious Transaction Reports
TF	Terrorist Financing
VA/VAs	Virtual Assets
VASPs	Virtual Asset Service Providers

Introduction

1. Virtual assets (VA) and related services have the potential to spur financial innovation and efficiency, but their distinct features also create new opportunities for money launderers, terrorist financiers, and other criminals to launder their proceeds or finance their illicit activities. The ability to transact across borders rapidly not only allows criminals to acquire, move, and store assets digitally often outside the regulated financial system, but also to obfuscate the origin or destination of the funds and make it harder for reporting entities to identify suspicious activity in a timely manner. These factors add hurdles to the detection and investigation of criminal activity by national authorities.
2. In October 2018, the Financial Action Task Force (FATF) updated its Standards to clarify the application of the FATF Standards to VA activities and Virtual Asset Service Providers (VASPs) in order to, among other things, assist jurisdictions in mitigating the money laundering (ML) and terrorist financing (TF) risks associated with VA activities and in protecting the integrity of the global financial system. In June 2019, the FATF adopted an Interpretative Note to Recommendation 15 to further clarify the application of FATF requirements to VA activities or operations and VASPs, including with respect to suspicious transaction reporting.
3. The FATF has prepared this brief report on ML/TF red flag indicators associated with VAs to assist reporting entities, including financial institutions (FIs), designated non-financial businesses and professions (DNFBPs), and VASPs; however, they are categorised, in identifying and reporting potential ML and TF activity involving VAs. This report should also facilitate reporting entities' application of a risk-based approach to their Customer Due Diligence (CDD) requirements, which require knowing who their clients and the beneficial owners are, understanding the nature and purpose of the business relationship, and understanding the source of funds.
4. Operational agencies including Financial Intelligence Units (FIUs), law enforcement authorities (LEAs), and prosecutors may find this report a useful reference for analysing suspicious transaction reports (STRs) or improving detection, investigation, and confiscation of VAs involved in misuse.
5. Financial, DNFBP, and VASP regulators, on the other hand, may find these indicators useful when preparing STRs and monitoring for entities' compliance with AML/CFT controls. Where a reporting entity has information indicating the existence of one or more indicators without logical business explanation, but fails to file an STR despite a customer's inconsistent explanation or fails to seek clarification on the transaction, competent authorities may consider following up with the reporting entity taking into account the latter's business profile.

Methodology and sources used in drawing up the list of red flag indicators

6. The red flag indicators included in this report are based on more than one hundred case studies contributed by jurisdictions from 2017-2020, the findings of the *Confidential FATF Report on Financial Investigations Involving Virtual Assets* (June 2019) and the published *FATF Report Virtual Currencies Key Definitions and Potential AML/CFT Risks* (June 2014), as well as information on the misuse of VAs available in the public domain.

Trends in use of VAs for ML/TF purposes

The majority of VA-related offences focused on predicate or ML offences. Notwithstanding, criminals did make use of VAs to evade financial sanctions and to raise funds to support terrorism.

The types of offences reported by jurisdictions include ML, the sale of controlled substances and other illegal items (including firearms), fraud, tax evasion, computer crimes (e.g. cyberattacks resulting in thefts), child exploitation, human trafficking, sanctions evasion, and TF. Among these, the most common type of misuse is illicit trafficking in controlled substances, either with sales transacted directly in VAs or the use of VAs as an ML layering technique. The second most common category of misuse is related to frauds, scams, ransomware, and extortion. More recently, professional ML networks have started exploiting VAs as one of their means to transfer, collect, or layer proceeds.

Source: Case studies contributed by jurisdictions from 2017-2020

Issues to note when reading this Report

7. These indicators are specific to the nature of VAs and their associated financial activities, and are by no means exhaustive. Suspicious activities involving the use of VAs may also share similar traits with ML/TF activities involving the use of fiat currency, or other kinds of assets. Reporting entities should therefore consider the risks posed by their customers, products, and operations, as well as the presence of conventional risk indicators. Red flag indicators should always be considered in context.

8. Freestanding red flags such as those listed below can be developed or combined with information from operational agencies, which can in turn be further developed through a public-private partnership, in a cyclical, evolutionary process that takes into account the unique risk and context of a jurisdiction, customer type, or the reporting entity itself. The mere presence of a red flag indicator is not necessarily a basis for a suspicion of ML or TF, but could prompt further monitoring and examination. Ultimately, a client may be able to provide an explanation to justify the red flag indicator, business or economic purposes of a transaction.

9. When evaluating potential suspicious activity, competent authorities, FIs, DNFBPs, and VASPs should be mindful that some red flag indicators might be more readily observable during general transactional monitoring, while others may be more readily observable during transaction-specific reviews. The observation of one or more of the indicators is dependent on the business lines, products, or services that an institution or VASP offers and how it interacts with its customers. When one or more red flag indicators are present and with little or no indication of a legitimate economic or business purpose, the reporting entity may be more likely to develop a suspicion that ML or TF is occurring.¹ These indicators should not be the sole determinant of whether or not an STR should be filed. Reporting entities should consider filing of an STR if they know, suspect, or have reasonable grounds that ML/TF has been committed.

Red Flag Indicators

10. The following sections contain a collection of red flag indicators of suspicious VA activities or possible attempts to evade law enforcement detection, as identified through more than one hundred case studies collected since 2017 from across the FATF Global Network, literature reviews, and open source research. As previously mentioned, the existence of a single indicator does not necessarily indicate criminal activity. Often, it is the presence of multiple indicators in a transaction with no logical business explanation that raises suspicion of potential criminal activity. The presence of indicators should encourage further monitoring, examination, and reporting where appropriate.

Red Flag Indicators Related to Transactions

11. While VAs are still not widely used by the public, their use has caught on among criminals. The use of VAs for ML purposes first emerged over a decade ago, but VAs are becoming increasingly mainstream for criminal activity more broadly. This set of indicators demonstrates how red flags traditionally associated with transactions involving more conventional means of payment remain relevant to detecting potential illicit activity related to VAs.

Size and frequency of transactions

- Structuring VA transactions (e.g. exchange or transfer) in small amounts, or in amounts under record-keeping or reporting thresholds, similar to structuring cash transactions.
- Making multiple high-value transactions –
 - in short succession, such as within a 24-hour period;
 - in a staggered and regular pattern, with no further transactions recorded during a long period afterwards, which is particularly common in ransomware-related cases; or

¹ While a number of red flag indicators could apply to both instances of ML and TF, e.g. fundraising activities, financing of foreign terrorist fighters (FTFs), and purchase of weapons (e.g. on the darknet) using VAs, readers are encouraged to read in connection with the Confidential FATF Report on Detecting Terrorist Financing: Relevant Risk Indicators (June 2016) (restricted access to FATF Members).

- to a newly created or to a previously inactive account.
- Transferring VAs immediately to multiple VASPs, especially to VASPs registered or operated in another jurisdiction where –
 - there is no relation to where the customer lives or conducts business; or
 - there is non-existent or weak AML/CFT regulation.
- Depositing VAs at an exchange and then often immediately –
 - withdrawing the VAs without additional exchange activity to other VAs, which is an unnecessary step and incurs transaction fees;
 - converting the VAs to multiple types of VAs, again incurring additional transaction fees, but without logical business explanation (e.g. portfolio diversification); or
 - withdrawing the VAs from a VASP immediately to a private wallet. This effectively turns the exchange/VASP into an ML mixer.
- Accepting funds suspected as stolen or fraudulent -
 - depositing funds from VA addresses that have been identified as holding stolen funds, or VA addresses linked to the holders of stolen funds.

Case Study 1. Multiple immediate transfers of large amount of VAs to overseas VASPs

A local VASP submitted STRs following suspicions concerning the purchase of large amounts of VAs by various individuals and their subsequent immediate transfers to VASPs in a foreign jurisdiction. In various instances, the individuals shared the same residential address; and most of the VA addresses were accessed from the same IP address – indicating the potential use of money mules by professional money launderers to launder the illicit proceeds.

In addition, multiple layering of the fiat funds was arranged prior to the VA purchase by mules. To disguise the funds' origin, cash was first deposited into various accounts at different FIs across the jurisdiction. Those funds were then further transferred to various accounts held in the name of entities registered in the jurisdiction. Electronic payments were made into the accounts in smaller amounts. After that, funds were transferred to another group of accounts before reaching the mules' accounts held with local VASPs. VAs were immediately purchased and transferred to foreign VASPs. More than 150 individuals were involved in this case, responsible for transferring a total of about USD 108 352 900 (or BTC 11,960) to multiple VA accounts held by two overseas VASPs.

Source: South Africa

Case Study 2. Multiple VAs and multiple transfers to foreign VASPs

A local VA exchange reported that approximately KRW 400 million (EUR 301 170) was stolen from phishing victims and was ultimately exchanged for VAs as a layering technique. What triggered the reporting was the multiple high-value transactions transferred to a foreign VASP into one single wallet. The stolen funds in fiat currency were first exchanged to three different types of VAs and then deposited to the suspect's VA wallet held with a local VASP. The suspect then attempted to obfuscate the source of funds by transferring funds an additional 55 times through 48 separate accounts held in different local VASPs, and then to a different VA wallet located abroad.

Source: South Korea

Red Flag Indicators Related To Transaction Patterns

12. Similar to the above section, the red flags below illustrate how the misuse of VAs for ML/TF purposes could be identified through irregular, unusual, or uncommon patterns of transactions.

Transactions concerning new users

- Conducting a large initial deposit to open a new relationship with a VASP, while the amount funded is inconsistent with the customer profile.
- Conducting a large initial deposit to open a new relationship with a VASP and funding the entire deposit the first day it is opened, and that the customer starts to trade the total amount or a large portion of the amount on that same day or the day after, or if the customer withdraws the whole amount the day after. As most VAs have a transactional limit for deposits, laundering in large amounts could also be done through over-the-counter-trading.²
- A new user attempts to trade the entire balance of VAs, or withdraws the VAs and attempts to send the entire balance off the platform.

Case Study 3. Initial deposit inconsistent with customer profile

The presence of the following suspicious indicators prompted an FI (bank) to file an STR with authorities, leading to an ML investigation:

- transactions inconsistent with the profile of the account holder – in the first two days after a personal account had been created for a young individual, the account received deposits of a commercial nature from different legal persons in large amounts;
- transaction patterns – the deposited funds were immediately transferred to accounts of several VASPs (in one day) for VA purchase (Bitcoin);

² Over-the-counter trading refers to securities that are traded for companies that are not listed on a formal exchange, and via a broker-dealer network.

- customer profile – one of the ordering parties was known to the bank as a subject in a fraud case. The bank also provided IP addresses used for internet banking services to the authorities.

Based on an investigation, the personal account holder appeared to be a money mule recruited by criminals on a social media platform to help receive claimed payments for goods sold online. However, such funds appeared to have been deposited by other victim companies and were not payments for goods. The deposited funds were immediately transferred out from the personal bank account via several divided payments to another account held by a joint-stock company in Czech Republic, and were exchanged to VA (Bitcoin) held in several local VASPs. These VASPs were then immediately withdrawn from the account. In addition to filing an STR, the bank also suspended the suspicious transfers, which made subsequent seizure of funds possible.

The local VASP also noticed irregularities in the funds received and provided useful information to aid the investigation. The information included: circumstances where the VAs were purchased; transaction and other CDD information such as wallet address, copy of misused identification document for the purchase, and name of the alleged buyer. These allowed authorities to request additional information from the banks (e.g. bank statements).

Source: Czech Republic

Transactions concerning all users

- Transactions involving the use of multiple VAs, or multiple accounts, with no logical business explanation.
- Making frequent transfers in a certain period of time (e.g. a day, a week, a month, etc.) to the same VA account –
 - by more than one person;
 - from the same IP address by one or more persons; or
 - concerning large amounts.
- Incoming transactions from many unrelated wallets in relatively small amounts (accumulation of funds) with subsequent transfer to another wallet or full exchange for fiat currency. Such transactions by a number of related accumulating accounts may initially use VAs instead of fiat currency.
- Conducting VA-fiat currency exchange at a potential loss (e.g. when the value of VA is fluctuating, or regardless of abnormally high commission fees as compared to industry standards, and especially when the transactions have no logical business explanation).
- Converting a large amount of fiat currency into VAs, or a large amount of one type of VA into other types of VAs, with no logical business explanation.

Case Study 4. Transfers conducted in a recurrent time

A local FI (securities firm) filed an STR regarding unauthorised payments between the VA accounts of their broker and a foreign national. The securities firm reported the activity after it determined that the foreign national intended to make transfers totalling USD 4.8 million (two separate transactions that occurred six minutes apart on the same day), and filed an application to the broker for a trading account the next business day. The wallet was not hosted in the Cayman Islands. The STR reporting led to a successful information exchange with foreign FIUs and the successful return of most of the funds to the victim, as the online platform in a foreign jurisdiction had been able to freeze the suspect's account before the offence had been completed.

Source: Cayman Islands

Red Flag Indicators Related to Anonymity

13. This set of indicators draws from the inherent characteristics and vulnerabilities associated with the underlying technology of VAs. The various technological features below increase anonymity and add hurdles to the detection of criminal activity by LEAs. These factors make VAs attractive to criminals looking to disguise or store their funds. Nevertheless, the mere presence of these features in an activity does not automatically suggest an illicit transaction. For example, the use of a hardware or paper wallet may be legitimate as a way to secure VAs against thefts. Again, the presence of these indicators should be considered in the context of other characteristics about the customer and relationship, or a logical business explanation.

- Transactions by a customer involving more than one type of VA, despite additional transaction fees, and especially those VAs that provide higher anonymity, such as anonymity-enhanced cryptocurrency (AEC) or privacy coins.
- Moving a VA that operates on a public, transparent blockchain, such as Bitcoin, to a centralised exchange and then immediately trading it for an AEC or privacy coin.
- Customers that operate as an unregistered/unlicensed VASP on peer-to-peer (P2P) exchange websites, particularly when there are concerns that the customers handle huge amount of VA transfers on its customer's behalf, and charge higher fees to its customer than transmission services offered by other exchanges. Use of bank accounts to facilitate these P2P transactions.
- Abnormal transactional activity (level and volume) of VAs cashed out at exchanges from P2P platform-associated wallets with no logical business explanation.
- VAs transferred to or from wallets that show previous patterns of activity associated with the use of VASPs that operate mixing or tumbling services or P2P platforms.

- Transactions making use of mixing and tumbling services, suggesting an intent to obscure the flow of illicit funds between known wallet addresses and darknet marketplaces.
- Funds deposited or withdrawn from a VA address or wallet with direct and indirect exposure links to known suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, illegal activities (e.g. ransomware) and/or theft reports.
- The use of decentralised/unhosted, hardware or paper wallets to transport VAs across borders.
- Users entering the VASP platform having registered their Internet domain names through proxies or using domain name registrars (DNS) that suppress or redact the owners of the domain names.
- Users entering the VASP platform using an IP address associated with a darknet or other similar software that allows anonymous communication, including encrypted emails and VPNs. Transactions between partners using various anonymous encrypted communication means (e.g. forums, chats, mobile applications, online games, etc.) instead of a VASP.
- A large number of seemingly unrelated VA wallets controlled from the same IP-address (or MAC-address), which may involve the use of shell wallets registered to different users to conceal their relation to each other.
- Use of VAs whose design is not adequately documented, or that are linked to possible fraud or other tools aimed at implementing fraudulent schemes, such as Ponzi schemes.
- Receiving funds from or sending funds to VASPs whose CDD or know-your-customer (KYC) processes are demonstrably weak or non-existent.
- Using VA ATMs/kiosks –
 - despite the higher transaction fees and including those commonly used by mules or scam victims; or
 - in high-risk locations where increased criminal activities occur.

A single use of an ATM/kiosk is not enough in and of itself to constitute a red flag, but would if it was coupled with the machine being in a high-risk area, or was used for repeated small transactions (or other additional factors).

Case Study 5. Use of IP address associated with Darknet Marketplace – Alpha Bay

AlphaBay, the largest criminal darknet market dismantled by authorities in 2017, was used by hundreds of thousands of people to buy and sell illegal drugs, stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms, and toxic chemicals over a two-year span. The site operated as a hidden service on the TOR network to conceal the locations of its underlying servers as well as the identities of its administrators, moderators, and users. AlphaBay vendors used a number of different types of VAs, and had approximately 200 000 users, 40 000 vendors, 250 000 listings and facilitated more than USD 1 billion in VA transactions between 2015 and 2017.

In July 2017, the U.S. Government, with assistance from foreign counterparts, took down the servers hosting the AlphaBay marketplace, arrested the administrator, and pursuant to a seizure warrant issued in the Eastern District of California, seized the physical and virtual assets from the marketplace itself, and those that represented the unlawful proceeds from the AlphaBay criminal enterprise. Federal agents obtained the warrants after tracing VAs transactions originating from AlphaBay to other VA accounts and identifying bank accounts and other tangible assets controlled by the alleged administrator.

Source: United States

Case Study 6. Use of mixing and tumbling – Helix

A darknet-based VASP, Helix, provided a mixing or tumbling service that helped customers conceal the source or owners of VAs for a fee over a three-year period. Helix allegedly transferred over 350,000 Bitcoin, with a value at the time of transmission of over USD 300 million. The operator specifically advertised the service as a way to conceal transactions on the darknet from law enforcement. In February 2020, criminal charges including ML conspiracy and operating an unlicensed money transmitting business were brought against an individual who operated Helix.

Helix partnered with the darknet marketplace AlphaBay until AlphaBay's seizure by law enforcement in 2017.

Source: United States

Case Study 7. Use of decentralised wallet

This case demonstrates how criminals make use of decentralised wallet to obfuscate the source of illicit funds generated from illicit drug trafficking activities. In this case, criminals conducted a large quantity of drug sales on the Internet and sought payment not only in fiat currency but also in the form of VAs (Bitcoin, EX-codes, EXMO-cheques).

Illicit funds received in fiat currency were converted to VA with the aid of an anonymous account at an online Blockchain trading platform. Such funds, in the form of VAs, were then converted back into fiat currency via an exchanger, before being transferred back to the criminals' personal bank card accounts. As for those illicit funds received in the form of VAs, they were first transferred to decentralised Bitcoin wallets held by the criminals concerned, before being further transferred to other Bitcoin wallets at different exchanges. This increases the difficulty of tracing and tracking the funds. Similarly, the laundered funds (in VAs) were then converted back to fiat before being credited into the criminal's bank card accounts. The criminal was convicted and sentenced to seven years' imprisonment and a criminal fine after trial.

Source: Russian Federation

Red Flag Indicators about Senders or Recipients

14. This set of indicators is relevant to the profile and unusual behaviour of either the sender or the recipient of the illicit transactions.

Irregularities observed during account creation

- Creating separate accounts under different names to circumvent restrictions on trading or withdrawal limits imposed by VASPs.
- Transactions initiated from non-trusted IP addresses, IP addresses from sanctioned jurisdictions, or IP addresses previously flagged as suspicious.
- Trying to open an account frequently within the same VASP from the same IP address.
- Regarding merchants/corporate users, their Internet domain registrations are in a different jurisdiction than their jurisdiction of establishment or in a jurisdiction with a weak process for domain registration.

Irregularities observed during CDD process

- Incomplete or insufficient KYC information, or a customer declines requests for KYC documents or inquiries regarding source of funds.
- Sender / recipient lacking knowledge or providing inaccurate information about the transaction, the source of funds, or the relationship with the counterparty.
- Customer has provided forged documents or has edited photographs and/or identification documents as part of the on-boarding process.

Case Study 8. Customer refusing to provide information on source of funds

An FI (bank) filed an STR concerning an account of a local company that held funds generated by the sale of coupons that can be traded with a product (bioplastics in this case). The funds were deposited by both natural and legal persons, with some originally in VAs. Despite further inquiries by the bank, representatives of the account holder did not provide information on the origins of the funds. Subsequent analysis by the authorities indicated that the funds sent by the company showed links with subjects connected to organised crime and with funds received from a fraudulent project.

Source: Italy

Profile

- A customer provides identification or account credentials (e.g. a non-standard IP address, or flash cookies) shared by another account.
- Discrepancies arise between IP addresses associated with the customer's profile and the IP addresses from which transactions are being initiated.
- A customer's VA address appears on public forums associated with illegal activity.
- A customer is known via publicly available information to law enforcement due to previous criminal association.

Case Study 9. Customer profile does not match with regular high-value VA trading

A VASP (exchanger) and an FI (payment institute) filed STRs with the FIU concerning a high value of VA trading that began when the account at the exchanger was opened. Specifically, the account holder had been carrying out various VA buying and selling transactions for over EUR 180 000 – which did not match the profile of the account holder (including occupation and salary).

Analysis found that the VAs were subsequently used for (i) transactions on a darknet market; (ii) online betting; (iii) transactions with VASPs that did not have adequate AML/CFT controls or that were under previous ML investigations involving millions of dollars; (iv) operations on platforms that offered peer-to-peer transactions of VAs; and (v) "mixing". The account holder had also made use of a variety of different means (e.g. money transfer, online banking, and prepaid cards) to move a consistent amount of funds out of his account in the same time frame. The funds received by the account holder appeared to come from a network of individuals who bought VAs (Bitcoin) in cash and were located in different jurisdictions in Asia and Europe (including Italy),

both via money transfer and the banking system. He also received funds on his prepaid cards from subjects in Africa and the Middle East, who in turn collected funds from fellow citizens residing in Italy and abroad. These funds were then used for cross-border transfers and online gambling, and were withdrawn in cash from ATMs in Italy.

Source: Italy

Profile of potential money mule or scam victims

- Sender does not appear to be familiar with VA technology or online custodial wallet solutions. Such persons could be money mules recruited by professional money launderers, or scam victims turned mules who are deceived into transferring illicit proceeds without knowledge of their origins.
- A customer significantly older than the average age of platform users opens an account and engages in large numbers of transactions, suggesting their potential role as a VA money mule or a victim of elder financial exploitation.
- A customer being a financially vulnerable person, who is often used by drug dealers to assist them in their trafficking business.
- Customer purchases large amounts of VA not substantiated by available wealth or consistent with his or her historical financial profile, which may indicate money laundering, a money mule, or a scam victim.

Case Study 10. Scam victims turned mules

In these investment scams, foreign nationals contacted pensioners and generally older persons by direct phone calls, emails, or through social media, and offered them investment opportunities in Bitcoin or other VAs with the promise to generate huge profits due to rising popularity in VAs and their increase in price. The initial investment in small amounts (in many cases no more than EUR 250) was made from the victims' bank account, credit card or via other means to various payment services and then ending up in the hands of the criminals. Alternatively, victims were instructed to exchange fiat currency to Bitcoin using a VA ATM and send the funds to an address specified by the criminals.

Victims were technologically not very adept and did not generally understand the VA technology or what they were really investing in. Criminals also asked victims to install a remote desktop application on their device so that the criminals could help transfer the funds correctly to specific accounts. This compromised the victims' devices so that the criminals could conduct unauthorised money transfers without the victim being aware of it until he/she noticed money missing from the account. In some cases, criminals also fabricated articles claiming that famous celebrities or wealthy businesspeople or newscasters were promoting VA investments, thereby giving victims a sense of trust and legitimacy to the "investments".

Source: Finland

Other unusual behaviour

- A customer frequently changes his or her identification information, including email addresses, IP addresses, or financial information, which may also indicate account takeover against a customer.
- A customer tries to enter into one or more VASPs from different IP addresses frequently over the course of a day.
- Use of language in VA message fields indicative of the transactions being conducted in support of illicit activity or in the purchase of illicit goods, such as drugs or stolen credit card information.
- A customer repeatedly conducts transactions with a subset of individuals at significant profit or loss. This could indicate potential account takeover and attempted extraction of victim balances via trade, or ML scheme to obfuscate funds flow with a VASP infrastructure.

Red Flag Indicators in the Source of Funds or Wealth

15. As demonstrated by cases submitted by jurisdictions, the misuse of VAs often relates to criminal activities, such as illicit trafficking in narcotics and psychotropic substances, fraud, theft and extortion (including cyber-enabled crimes). Below are common red flags related to the source of funds or wealth linked to such criminal activities:

- Transacting with VA addresses or bank cards that are connected to known fraud, extortion, or ransomware schemes, sanctioned addresses, darknet marketplaces, or other illicit websites.
- VA transactions originating from or destined to online gambling services.
- The use of one or multiple credit and/or debit cards that are linked to a VA wallet to withdraw large amounts of fiat currency (crypto-to-plastic), or funds for purchasing VAs are sourced from cash deposits into credit cards.
- Deposits into an account or a VA address are significantly higher than ordinary with an unknown source of funds, followed by conversion to fiat currency, which may indicate theft of funds.
- Lack of transparency or insufficient information on the origin and owners of the funds, such as those involving the use of shell companies or those funds placed in an Initial Coin Offering (ICO) where personal data of investors may not be available or incoming transactions from online payments system through credit/pre-paid cards followed by instant withdrawal.
- A customer's funds which are sourced directly from third-party mixing services or wallet tumblers.
- Bulk of a customer's source of wealth is derived from investments in VAs, ICOs, or fraudulent ICOs, etc.
- A customer's source of wealth is disproportionately drawn from VAs originating from other VASPs that lack AML/CFT controls.

Case Study 11. Use of shell companies – Deep Dot Web

In May 2019, U.S. LEAs seized a website, DeepDotWeb (DDW), pursuant to a court order. The alleged owners and operators of DDW were charged in an ML conspiracy related to millions of dollars in kickbacks they received for referring individuals to darknet marketplaces from the DDW website. Through referral links, the alleged owners and operators of DDW received kickback payments, representing commissions on the proceeds from the purchase of illegal goods, such as fentanyl and heroin, made by individuals referred to a darknet marketplace from the DDW site.

These kickback payments were made in VA and paid into a DDW-controlled Bitcoin wallet. To conceal and disguise the nature and source of the illegal proceeds, which totalled over USD 15 million, the owners and operators transferred their illegal kickback payments from their DDW Bitcoin wallet to other Bitcoin wallets, as well as to bank accounts that they controlled in the names of shell companies. The defendants used these shell companies to move their ill-gotten gains and conduct other activity related to DDW. During a five-year period, the website received approximately 8 155 Bitcoin in kickback payments from darknet marketplaces, worth approximately USD 8 million, adjusted for the trading value of Bitcoin at the time of each transaction. The Bitcoin was transferred to DDW’s Bitcoin wallet, controlled by the defendants, in a series of more than 40 000 deposits, and was subsequently withdrawn to various destinations in over 2 700 transactions. The value of the Bitcoin at the time of the withdrawals from the DDW Bitcoin wallet equalled to approximately USD 15 million.

Source: United States

Case Study 12. Use of multiple VA exchanges, false identification documents for CDD and prepaid cards

The defendants in this matter allegedly operated an ML scheme in connection with cybercriminals who hacked a VA exchange and stole USD 250 million worth of VAs. The two defendants allegedly laundered about USD 91 million worth of the stolen VAs, as well as USD 9.5 million from another cyber theft.

The stolen VAs were then routed through hundreds of automated VA transactions and multiple VA exchanges. The launderers used doctored photographs and falsified identification documents in some cases to circumvent KYC procedures at the VA exchanges. Some USD 35 million of the illicit funds ultimately were transferred into foreign bank accounts and were also used to purchase prepaid cards, which could be exchanged for VAs. The defendants operated through independent as well as linked accounts and provided VA transmission services, such as

converting VAs into fiat currency, to customers for a fee. The defendants also conducted business in the US but at no time registered with the Financial Crimes Enforcement Network (FinCEN).

Source: United States

Red Flag Indicators Related to Geographical Risks

16. This set of indicators emphasises how criminals, when moving their illicit funds, have taken advantage of the varying stages of implementation by jurisdictions on the revised FATF Standards on VAs and VASPs.³ Based on cases reported by jurisdictions, criminals have exploited the gaps in AML/CFT regimes on VAs and VASPs by moving their illicit funds to VASPs domiciled or operated in jurisdictions with non-existent or minimal AML/CFT regulations on VAs and VASPs. These jurisdictions may not have a registration/licensing regime, or have not extended STR requirements to cover VAs and VASPs, or may not have otherwise introduced the full spectrum of preventive measures as required by the FATF Standards. While this report does not seek to identify a list of “high risk” jurisdictions, reporting entities are invited to take into account the following indicators when considering geographical risks. These risks are associated with source, destination, and transit jurisdictions of a transaction. They are also relevant to risks associated with the originator of a transaction and the beneficiary of funds that may be linked to a high-risk jurisdiction. In addition, they may be applicable to the customer’s nationality, residence, or place of business.

- Customer’s funds originate from, or are sent to, an exchange that is not registered in the jurisdiction where either the customer or exchange is located.
- Customer utilises a VA exchange or foreign-located MVTS in a high-risk jurisdiction lacking, or known to have inadequate, AML/CFT regulations for VA entities, including inadequate CDD or KYC measures.
- Customer sends funds to VASPs operating in jurisdictions that have no VA regulation, or have not implemented AML/CFT controls.
- Customer sets up offices in or moves offices to jurisdictions that have no regulation or have not implemented regulations governing VAs, or sets up new offices in jurisdictions where there is no clear business rationale to do so.

³ In July 2020, the FATF published a [12-Month Review of The Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers](#). Section 2 of the Report covers the progress of implementation of the revised Standards since June 2019.

Case Study 13. Bitcoin dealer operating unlicensed money transmitting businesses (cross-border elements)

In April 2019, the defendant received a sentence of two years in prison for operating an unlicensed money transmitting business after selling hundreds of thousands of dollars of VA (Bitcoin) to more than a thousand customers in the US. The defendant was also ordered to forfeit USD 823 357 in profits.

The defendant advertised his services on websites for VA users, meeting some customers in person to accept cash in exchange for VAs. Other customers paid him via nationwide ATMs or money transmitting services. The defendant received a five percent premium on the prevailing exchange rate for his services. He first acquired Bitcoin through a US exchange, but once his activities triggered suspicion and his account was closed, the defendant then switched to an exchange in Asia. Using that exchange, the defendant bought USD 3.29 million in Bitcoin, in hundreds of separate transactions, between March 2015 and April 2017. The defendant also admitted that he exchanged his US cash, which he kept in another jurisdiction bordering the US, with a precious metals dealer, and that between late 2016 and early 2018, he and others imported into the US a total of over USD 1 million, in amounts slightly below the USD 10 000 reporting requirement.

Source: United States

VASP moving its operation to a jurisdiction that has inadequate AML/CFT regulations

Ahead of the implementation of a policy to prohibit VASP operation in Jurisdiction A in Asia in 2017, a VASP (exchange) established in Jurisdiction A transferred its operation to Jurisdiction B in the same region. In 2018, Jurisdiction B stepped up its AML/CFT legal regime on VAs following significant hacks of some major VASPs (exchanges). In March 2018, the VASP announced its intentions to relocate its headquarters to Jurisdiction C in Europe (a jurisdiction which had not yet introduced a comprehensive AML/CFT regime in relation to VAs and VASPs at the time). Later in November 2018, Jurisdiction C introduced certain regulations on VASPs, and in February 2020, it confirmed that no authorisation was given to the corresponding VASP to operate. More recent reports in 2020 indicated that the VASP had already relocated its registration and domicile status to Jurisdiction D in Africa.

Source: Public domain

Conclusion

17. This Report is drawn from extensive input by FATF Members across the global network, and seeks to provide a practical tool for both the public and private sectors in identifying, detecting, and ultimately preventing criminal, ML, and TF activities involving VAs.

18. The indicators included in this Report are specific to the inherent characteristics and vulnerabilities associated with VAs. They are neither exhaustive nor applicable in every situation. The indicators are often just one of many elements contributing to a bigger overall picture of potential ML or TF risk and it is important that the indicators (or any single indicator) not be viewed in isolation. They should be contextualised with information obtained from relevant authorities.

19. A risk-based approach implemented with a regular and dynamic two-way dialogue between the public and private sectors would no doubt enhance the effectiveness of this Report. Competent authorities are therefore encouraged to disseminate this Report to reporting entities, and to conduct engagement and awareness-raising sessions with them to promote their understanding of this Report.

20. While the indicators identified are constantly evolving, they are best used when applying other contextual information from domestic law enforcement and public sources. Competent authorities may also provide private sectors with the indicators and information most relevant for that jurisdiction. For example, using the information in this Report to prepare their own advisories to relevant reporting entities. However, this Report should not be intended for use as a regulatory tool for compliance and examination purposes, or as a checklist when supervising private sector institutions as not all indicators are applicable to all jurisdictions or all institutions.

References

FATF (June 2014), [FATF Report Virtual Currencies Key Definitions and Potential AML/CFT Risks](#)

FATF (June 2019), [FATF Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers](#)

FATF (June 2020), [12-month Review of Revised FATF Standards – Virtual Assets and VASPs](#)

Reports restricted to FATF Members

FATF (June 2016), [Confidential FATF Report on Detecting Terrorist Financing: Relevant Risk Indicators](#)

FATF (June 2019), [Confidential FATF Report on Financial Investigations Involving Virtual Assets](#)

Virtual Assets - Red Flag Indicators of Money Laundering and Terrorist Financing

Virtual assets and related services have the potential to spur financial innovation and efficiency, but their distinct features also create new opportunities for money launderers, terrorist financiers, and other criminals to launder their proceeds or finance their illicit activities

The FATF has prepared this brief report on red flag indicators associated with virtual assets to assist reporting entities, including financial institutions, designated non-financial businesses and professions, and virtual asset service providers, in identifying and reporting potential money laundering and terrorist financing activity involving virtual assets.



REPORT OF THE
ATTORNEY
GENERAL'S
**CYBER
DIGITAL**
TASK FORCE

CRYPTOCURRENCY

**ENFORCEMENT
FRAMEWORK**

REPORT OF THE
ATTORNEY
GENERAL'S
**CYBER
DIGITAL
TASK FORCE**

United States Department of Justice
Office of the Deputy Attorney General
Cyber-Digital Task Force
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530
<https://www.justice.gov/cryptoreport>

October 2020

* * *

Guidance Disclaimer: This document does not contain any new binding legal requirements not otherwise already imposed by statute or regulation. To the extent this Enforcement Framework is viewed as a guidance document within the definition of Executive Order 13891, the contents of this document do not have the force and effect of law and are not meant to bind the public in any way. If viewed as a guidance document, this document is intended only to provide clarity to the public regarding existing requirements under the law or Department of Justice policies.

TABLE OF CONTENTS

ATTORNEY GENERAL’S CYBER-DIGITAL TASK FORCE	v
INTRODUCTION.....	vii
CRYPTOCURRENCY: AN ENFORCEMENT FRAMEWORK.....	1
PART I	
THREAT OVERVIEW	2
THE BASICS	2
LEGITIMATE USES	5
ILLICIT USES.....	5
THE ROLE OF DARKNET MARKETS.....	16
PART II	
LAW AND REGULATIONS	20
CRIMINAL CODE AUTHORITIES	20
REGULATORY AUTHORITIES.....	22
INTERNATIONAL REGULATION	35
PART III	
ONGOING CHALLENGES AND FUTURE STRATEGIES.....	37
BUSINESS MODELS AND ACTIVITIES THAT MAY FACILITATE CRIMINAL ACTIVITY.....	37
DEPARTMENT OF JUSTICE RESPONSE STRATEGIES	44
CONCLUSION.....	51



ATTORNEY GENERAL'S CYBER-DIGITAL TASK FORCE

TASK FORCE MEMBERS

Sujit Raman, Chair

Associate Deputy Attorney General
Office of the Deputy Attorney General

John Brown

Executive Assistant Director
Federal Bureau of Investigation

Brian C. Rabbitt

Assistant Attorney General (Acting)
Criminal Division

John C. Demers

Assistant Attorney General
National Security Division

Terry Wade

Executive Assistant Director
Federal Bureau of Investigation

Andrew E. Lelling

United States Attorney
District of Massachusetts

Beth A. Williams

Assistant Attorney General
Office of Legal Policy

TASK FORCE CONTRIBUTORS

Anthony M. Shults

Senior Counsel, Office of Legal Policy
Staff Director

Sabrina Bagdasarian

Jeff Breinholt

Thomas Burrows

Richard W. Downing

Lindsey Freeman

Christopher Hardee

Adam Hickey

Michele R. Korver

Erin Mikita

Sean Newell

C. Alden Pelker

Kimberley Raleigh

Leo Tsao

And the Men and Women of the Federal Bureau of Investigation

INTRODUCTION

Innovation can drive a society forward. But innovation does not occur in a vacuum. Public policy can establish background conditions that help the innovative spirit thrive—or create an environment in which that spirit is inhibited, or suppressed.

Even in societies where transformative scientific and technological advancements are achievable, public policy again plays a critical mediating role. In the wrong hands, or without appropriate safeguards and oversight, these advancements can facilitate great human suffering. Just ask the political enemies of authoritarian regimes that deploy surveillance tools Orwell never could have imagined. Or, closer to home, listen to the child victims of unspeakable sexual exploitation whose images and livestreamed abuse are so easily transmitted across the internet.

Technological innovation and human flourishing are complementary concepts, but the former does not guarantee the latter. Good public policy—and the fair and equitable enforcement of such policy—can help bring the two into alignment. And even as too much regulation undoubtedly stifles innovation (and human flourishing, too), the absence of law’s protections can endanger progress across both dimensions. It takes careful consideration, and a deep and ongoing immersion in the facts, to understand when, and how, law should intervene. Once law’s empire has established its root in a particular domain, it requires equally careful consideration (and humility on the part of government officials) to

ensure that regulation goes no further than is required—that government action, in other words, reflects enforcement only of “those wise restraints that make us free.”ⁱ

This Enforcement Framework

In 2018, Attorney General Jeff Sessions established a Cyber-Digital Task Force within the U.S. Department of Justice to evaluate the impact that recent advances in technology have had on law enforcement’s ability to keep our citizens safe. Acknowledging the many ways in which technological advances “have enriched our lives and have driven our economy,” the Attorney General also noted that “the malign use of . . . technolog[y] harms our government, victimizes consumers and businesses, and endangers public safety and national security.”ⁱⁱ

The Task Force issued a comprehensive report later that year. That report identified particular threats currently confronting our society, ranging from transnational criminal enterprises’ sophisticated cyber-enabled schemes, to malign foreign influence operations, to efforts to compromise our nation’s critical infrastructure. The report also identified a number of emerging threats whose contours are still developing, and recommended further examination of their potential impact. Specifically, the report recommended that “the Department should continue evaluating the emerging threats posed by rapidly developing cryptocurrencies that malicious cyber actors often use.”ⁱⁱⁱ This Cryptocurrency Enforcement Framework represents the fruits of the Task Force’s efforts.

At the outset, it bears emphasizing that distributed ledger technology, upon which all cryptocurrencies build, raises breathtaking possibilities for human flourishing. These possibilities are rightly being explored around the globe, from within academia and industry, and from within governments—including our own.

It should be no surprise, for example, that researchers within the U.S. National Institute of Standards and Technology “have been investigating blockchain technologies at multiple levels: from use cases, applications and existing services, to protocols, security guarantees, and cryptographic mechanisms.”^{iv} Or that the U.S. Department of Defense’s recently-issued Digital Modernization Strategy specifically identifies blockchain technology as having “promise to provide increased effectiveness, efficiency, and security.”^v Or that the U.S. Food and Drug Administration recently released a detailed vision for how it plans to deploy blockchain for food safety-related purposes.^{vi} Or that—in the cryptocurrency space specifically—“the Federal Reserve is active in conducting research and experimentation related to distributed ledger technologies and the potential use cases for digital currencies,” including by partnering with the Massachusetts Institute of Technology to “build and test a hypothetical digital currency oriented to central bank uses.”^{vii} Without doubt, cryptocurrency represents a transformative way to store and exchange value.

But as the following pages make clear, despite its relatively brief existence, this technology already plays a role in many of the most significant criminal and national security

threats our nation faces. As the Task Force has found, illicit uses of cryptocurrency typically fall into three categories: (1) financial transactions associated with the commission of crimes; (2) money laundering and the shielding of legitimate activity from tax, reporting, or other legal requirements; or (3) crimes, such as theft, directly implicating the cryptocurrency marketplace itself. Part I of this Enforcement Framework examines in detail each of those categories.

Our society is not powerless in the face of these threats. As Part II demonstrates, the government has legal and regulatory tools available at its disposal to confront the threats posed by cryptocurrency’s illicit uses. Interagency partnership is critical for effectively leveraging those tools. The Department of Justice has built strong working relationships with its regulatory and enforcement partners in the Securities and Exchange Commission, the Commodity Futures Trading Commission, and the U.S. Department of the Treasury (including FinCEN, OFAC, and the IRS), among others, to enforce federal law in both its civil and criminal aspects. We have actively participated in international regulatory and criminal enforcement efforts, as well.

Those efforts are paying off. The past year alone has witnessed the indictment and arrest of the alleged operator of the world’s largest online child sexual exploitation market, involving an enforcement action that was coordinated with the disruption of that darknet market, the rescue of over 20 child victims, and the seizure of hundreds of thousands of dollars’ worth of bitcoin; the largest-ever seizure of cryptocurrency in the terrorism context, stemming from the

dismantling of terrorist financing campaigns running into the millions of dollars involving Hamas’s military wing, al-Qaeda, and ISIS; the first-ever imposition of economic sanctions for virtual-asset-related malicious cyber activity; and a novel (and successful) use of the federal securities laws to protect investors in the cryptocurrency space, resulting in the disgorgement of over \$1.2 billion in ill-gotten gains in a single case. We expect these enforcement trends to continue.

This report concludes in Part III with a discussion of the ongoing challenges the government faces in cryptocurrency enforcement—particularly with respect to business models (employed by certain cryptocurrency exchanges, platforms, kiosks, and casinos), and to activity (like “mixing” and “tumbling,” “chain hopping,” and certain instances of jurisdictional arbitrage) that may facilitate criminal activity.

The Challenges We Face

Those challenges map neatly onto the broader set of challenges that many emerging technologies present to law enforcement. Blockchain-related technologies are complex and are difficult to learn; for example, the methods for executing crimes like pump-and-dump schemes are changing, and require investigators to familiarize themselves with everything from how initial coin offerings (ICOs) are conducted to how technologically-savvy people communicate on specialized communications applications. Not only are these emerging technologies difficult to learn, but the relevant markets also rapidly evolve. The ICO boom from a few years ago has given way to the exponential growth of Decentralized Finance markets in recent

months—with all the associated complexities and difficulties for enforcers seeking to stay ahead of the curve and keep investors safe.

The global nature of the blockchain ecosystem adds a further layer of complexity. Crime has been expanding beyond national borders for years, but blockchain takes this globalization to another level. Parties conduct transactions and transfers between continents in a matter of minutes, and the digital infrastructure of the blockchain itself almost always transcends territorial boundaries. Adding to the difficulty, some of the largest cryptoasset exchanges operate outside of the United States, and many still require nothing more than an unverified email address before allowing an individual to begin trading. Finally, decentralized platforms, peer-to-peer exchangers, and anonymity-enhanced cryptocurrencies that use non-public or private blockchains all can further obscure financial transactions from legitimate scrutiny. As this Enforcement Framework makes clear, the challenges are significant. But so, too, are the resources that the U.S. Department of Justice, as well as the U.S. government as a whole, are dedicating to the effort, in collaboration with our international partners.

The Web 3.0

Technologists often talk about the Web 3.0, the next phase of the internet’s evolution. On this vision, humans will reclaim the internet, their data, and their anonymity from large outside forces, whether they be corporate firms or government entities. Cryptocurrency—a medium of exchange defined, at its core, by a sense of private, individual control, and whose underlying

blockchain technology already provides the backbone for applications outside the digital currency context—is central to this decentralized, anonymized, and still-being-defined notion of a future in which “a more semantically intelligent web” leverages data that “will be used by algorithms to improve user experience and make the web more personalized and familiar,” and in which users will no longer have to “rely on network and cellular providers that surveil the information going through their systems.”^{viii} Ultimately, the Web 3.0 is a vision about the nature of data itself, foretelling a world in which information is diffuse and dynamic—present everywhere at once, and therefore beyond any outsider’s grasp.

Only time will tell how, and in what form, the Web 3.0 finally takes shape. To its proponents, this vision marries technological innovation

with human flourishing. This Enforcement Framework suggests that, however liberating the emerging glimpses of the Web 3.0 might seem to be, that vision also can pose uniquely dangerous threats to public safety. Confronting and addressing those threats is what good public policy should do—and what the crypto ecosystem itself may have to do, if its vision of the future is ever fully to take hold. Meanwhile, federal authorities will continue vigorously enforcing the law as it exists, and pursuing justice on behalf of the American people.



– **Sujit Raman**, *Chair,*
Attorney General’s Cyber-Digital Task Force



Deputy Attorney General Jeffrey A. Rosen announces on September 22, 2020 the results of Operation DisrupTor, the U.S. government’s largest operation to date targeting criminal activity on the darknet. The operation resulted in the arrest of nearly 180 dark web drug traffickers and criminals; the seizure of approximately 500 kilograms of illegal drugs worldwide; and the seizure of millions of dollars in cash and virtual currencies.

CRYPTOCURRENCY: AN ENFORCEMENT FRAMEWORK

Innovations in technology often change the world for the better. And yet, criminals, terrorists, and rogue states can use those same innovations for their own illegitimate ends, imposing great costs on the public. Today, few technologies are more potentially transformative and disruptive—and more potentially susceptible to abuse—than cryptocurrency.

Cryptocurrency is a form of virtual asset that uses cryptography to secure financial transactions. Many of cryptocurrency's central features—including decentralized operation and control, and, in some cases, a high degree of anonymity—present new and unique challenges for public safety that must be addressed, lest the technology be used predominantly for criminal activity. Indeed, despite its relatively brief existence, cryptocurrency technology plays a role in many of the most significant criminal and national security threats that the United States faces. For example, cryptocurrency is increasingly used to buy and sell lethal drugs on the dark web (and by drug cartels seeking to launder their profits), contributing to a drug epidemic that killed over 67,000 Americans by overdose in 2018 alone.¹ Rogue states like Russia, Iran, and North Korea may turn to cryptocurrency to fund cyber-attacks, blunt the impact of U.S. and international sanctions, and decrease America's influence in the global marketplace. And, while terrorist use of cryptocurrency is still evolving, certain terrorist groups have solicited cryptocurrency donations running into the millions of dollars via online social media campaigns.

The U.S. Department of Justice is responsible for investigating and prosecuting crimes and threats to national security, including those facilitated by the use of cryptocurrency. As consumers, investors, financial institutions, elected officials, and other stakeholders consider the future path of cryptocurrency and related technologies, we are publishing this Framework to enhance understanding of the associated public safety and national security challenges that these technologies present. These challenges impact the security and legitimacy of the cryptocurrency ecosystem itself; only by identifying and responsibly addressing them can the risks of cryptocurrency be mitigated. At a minimum, this means that entities that use or are impacted by cryptocurrency must understand their legal obligations and invest in meeting them. For example, cryptocurrency exchanges—including those physically located outside the United States—must take seriously their legal and regulatory obligations, discussed in greater detail below, to protect users and to safeguard potential evidence in criminal or national security investigations. Where a breach of these obligations might rise to the level of a criminal violation, the Department will take appropriate action.

In the pages that follow, we:

(1) describe how cryptocurrency technology is currently used and illustrate how malicious actors have misused that technology to harm cryptocurrency users, exchanges, and investors, as well as to facilitate a broad range of crimes from child exploitation to terrorism;

(2) identify some of the key legal authorities and partnerships the Department has relied upon to combat criminal and national security threats involving cryptocurrency; and

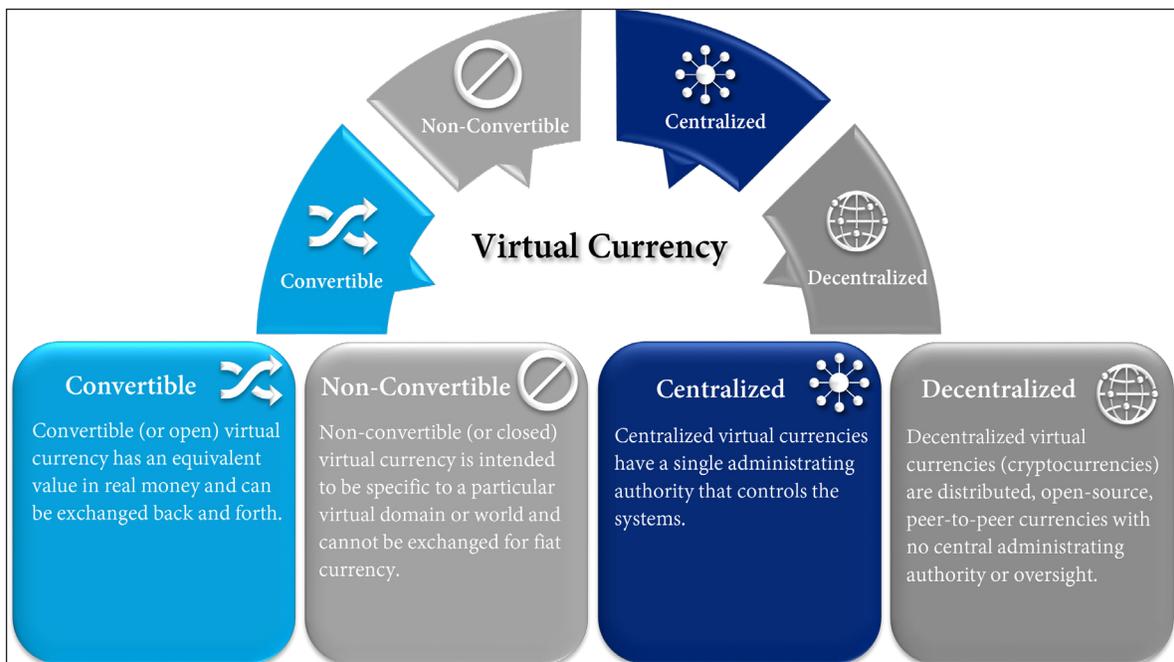
(3) discuss approaches for addressing the growing public safety challenges related to cryptocurrency.

I. Threat Overview

A. The Basics

“Virtual currency” is a digital representation of value that, like traditional coin and paper currency, functions as a medium of exchange—i.e., it can be digitally traded or transferred, and can be used for payment or investment purposes. Virtual currency is a type of “virtual asset” that is separate and distinct from digital representations of traditional currencies, securities, and other traditional financial assets.² Moreover, unlike “traditional currency”—which is also referred to as fiat currency, real currency, or national currency—virtual currency does not have legal tender status in any particular country or for any government or other

Figure 1: Systemic Attributes of Virtual Currency



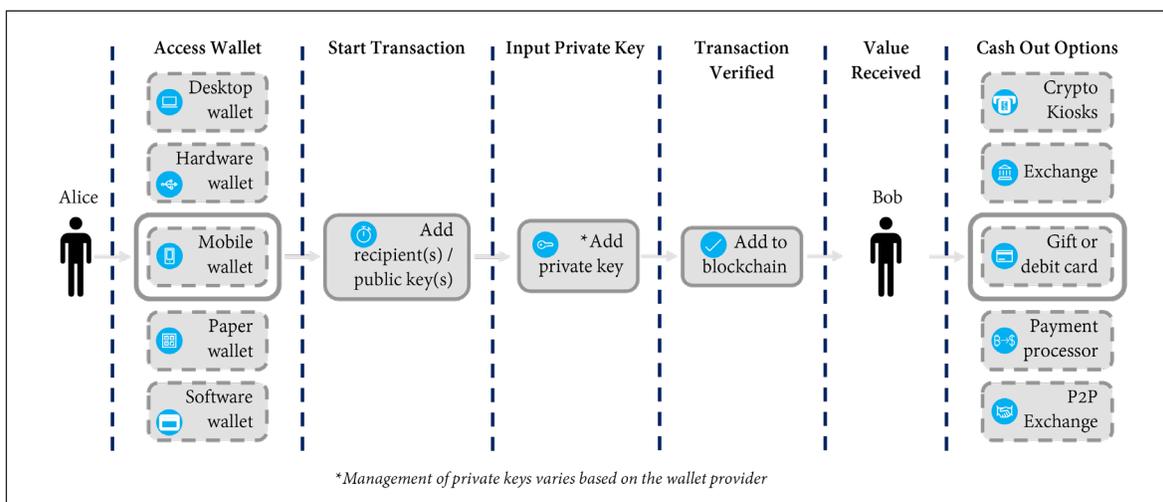
creditor.³ Instead, the exchange value of a particular virtual currency generally is based on agreement or trust among its community of users. Virtual currency can be *convertible*, meaning it has an equivalent value in real currency or acts as a substitute for real currency, or *non-convertible*, meaning it is specific to a particular virtual domain—such as an online gaming community—and cannot be exchanged for real currency.⁴

“Cryptocurrency” refers to a specific type of virtual currency with key characteristics. The vast majority of cryptocurrencies are decentralized, as they lack a central administrator to issue currency and maintain payment ledgers—in other words, there is no central bank. Instead, cryptocurrencies rely on complex algorithms, a distributed ledger that is often referred to as the “blockchain,” and a network of peer-to-peer users to maintain an accurate system of payments and receipts. As their name suggests, cryptocurrencies rely on cryptography for

security. Some examples of cryptocurrencies include Bitcoin,⁵ Litecoin, and Ether.

Cryptocurrency can be exchanged directly person to person; through a cryptocurrency exchange; or through other intermediaries. The storage of cryptocurrency is typically associated with an individual “wallet,” which is similar to a virtual account. Wallets can interface with blockchains and generate and/or store the public keys (which are roughly akin to a bank account number) and private keys (which function like a PIN or password) that are used to send and receive cryptocurrency. Cryptocurrency wallets can be housed in a variety of forms, including on a tangible, external device (“hardware wallets”); downloaded as software (“software wallets”) onto either a personal computer or server (“desktop wallets”) or an application on a smartphone (“mobile wallets”); as printed public and private keys (“paper wallets”); and as an online account associated with a cryptocurrency exchange.

Figure 2: Anatomy of a Cryptocurrency Transaction

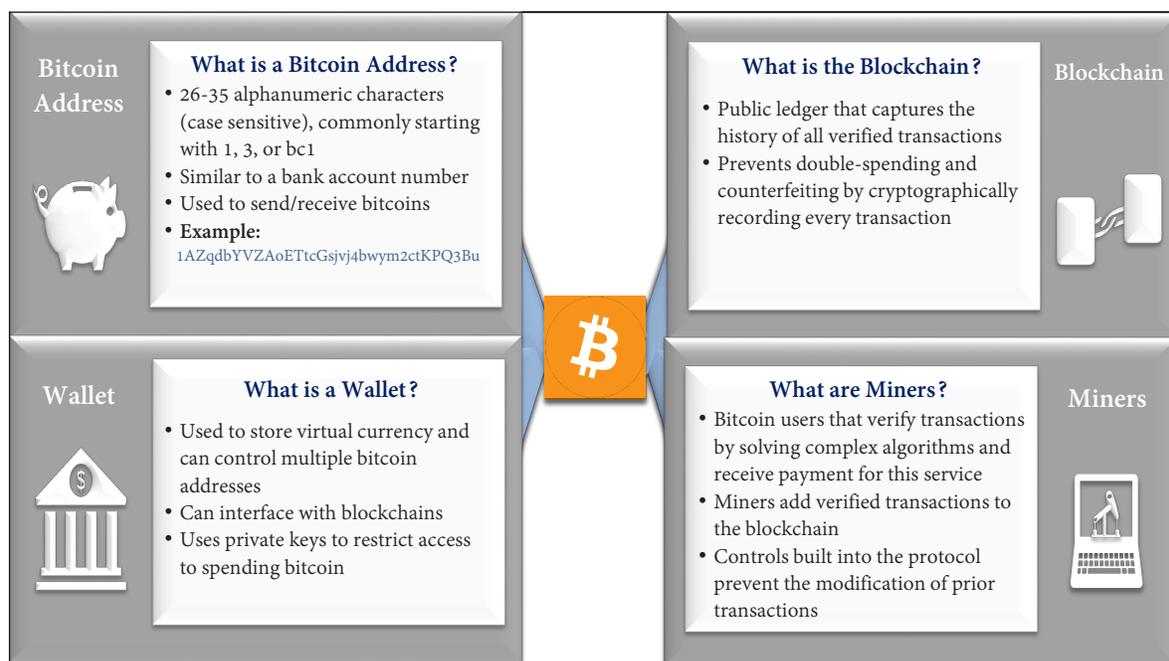


The distributed ledger—which, as noted above, is known as the “blockchain” for most cryptocurrencies—allows such a decentralized system to accurately track payments and to prevent double-spending and counterfeiting by cryptographically recording every transaction. When a transaction is initiated, it is shared with participants on the network associated with

payment in the cryptocurrency itself—a process known as “mining.”

Cryptocurrencies can vary in their degree of anonymity depending on the public or non-public nature of their associated blockchain. For instance, while Bitcoin addresses do not have names or specific customer information attached to them, Bitcoin’s blockchain is

Figure 3: Bitcoin Basics – Key Terms



the particular cryptocurrency, whereupon special users (often called “miners”) verify that the units have not already been spent, and validate the transaction by solving a complex algorithm. The transaction is then added to the blockchain, with each block consisting of a group of reported transactions in chronological order. In exchange for participating in this community validation process, miners generate and receive a

public. As a result, users can query addresses to view and understand Bitcoin transactions to some extent. Other cryptocurrencies, however, use non-public or private blockchains that make it more difficult to trace or to attribute transactions. These are often referred to as “anonymity enhanced cryptocurrencies” (“AECs”) or “privacy coins.” Examples of AECs include Monero, Zcash, and Dash.

B. Legitimate Uses

Cryptocurrency advocates maintain that a decentralized, distributed, and secure cryptocurrency holds great promise for legitimate use. Today's market includes over 2,000 cryptocurrencies, which enable users to transfer virtual currency around the globe in exchange for goods, services, and other sources of value. Proponents of cryptocurrency contend that, by eliminating the need for financial intermediaries to validate and facilitate transactions, cryptocurrency has the potential to minimize transaction costs and to reduce corruption and fraud. In addition, some users—particularly those in countries beset by rampant inflation and where access to normal foreign exchange is limited—may use virtual currency to avoid inflation in fiat currencies.

Some advocates also claim that cryptocurrency may in the future facilitate “micro-payments,” providing enterprises with the opportunity to sell low-cost goods and services that may not be profitable enough with traditional credit and debit, due to higher transaction costs. Others believe that cryptocurrency can provide new access to markets, including to individuals in the developing world who are not served by banks or other financial institutions. Cryptocurrency advocates also stress that the privacy associated with cryptocurrency, though raising significant challenges for law enforcement, can have valid and beneficial uses. For example, such advocates claim that greater anonymity may reduce the risk of account or identity theft associated with the use of traditional credit systems.

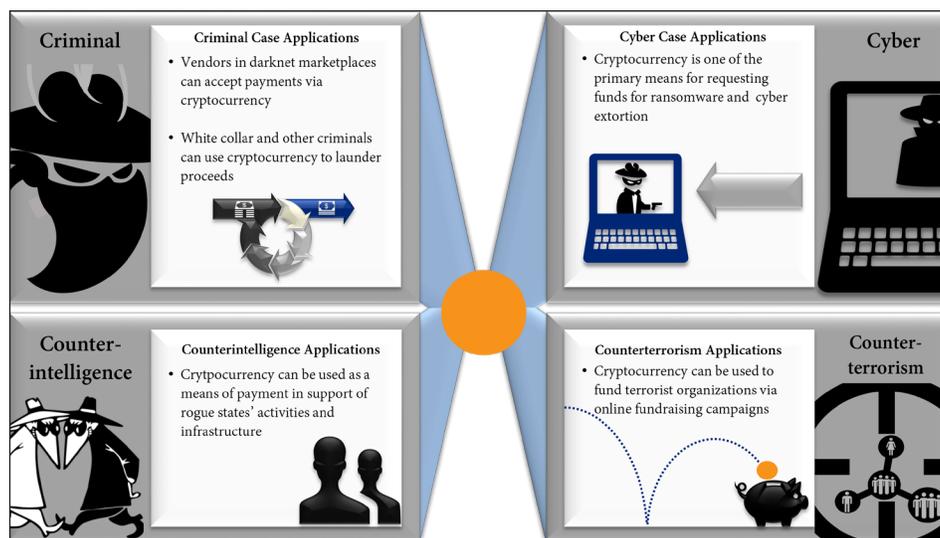
On the other hand, in addition to the substantial public safety and national security concerns discussed in this Framework, critics of cryptocurrency have raised questions about its supposed benefits. For example, certain critics contend that cryptocurrency could, if widely adopted, reduce the ability of national governments to regulate their economies through monetary policy. Others have raised concerns about the security of cryptocurrency wallets and exchanges, or pointed to the high volatility in value that most virtual currencies have experienced.

Whatever the overall benefits and risks of cryptocurrency, the Department of Justice seeks to ensure that uses of cryptocurrency are functionally compatible with adherence to the law and with the protection of public safety and national security.

C. Illicit Uses

Many crimes that involve the use of cryptocurrency—for example, buying and selling illicit drugs—are not new, but criminals increasingly are leveraging cryptocurrency's features to advance and conceal unlawful schemes. In general, the illicit use of cryptocurrency can fall into three broad categories. As explained further below, bad actors may exploit cryptocurrency to: (1) engage in financial transactions associated with the commission of crimes, such as buying and selling drugs or weapons on the dark web, leasing servers to commit cybercrimes, or soliciting funds to support terrorist activity; (2) engage in money laundering or shield otherwise legitimate activity from tax, reporting, or other legal requirements; or (3) commit crimes directly

Figure 4 : Examples of Cryptocurrencies in Investigations



implicating the cryptocurrency marketplace itself, such as stealing cryptocurrency from exchanges through hacking or using the promise of cryptocurrency to defraud unwitting investors.⁶

1. Using Cryptocurrency Directly to Commit Crimes or to Support Terrorism

Criminals use cryptocurrency to facilitate crimes and to avoid detection in ways that would be more difficult with fiat currency or “real money.” They can avoid large cash transactions and mitigate the risk of bank accounts being traced, or of banks notifying governments of suspicious activity. Criminals have used cryptocurrency, often in large amounts and transferred across international borders, as a new means to fund criminal conduct ranging from child exploitation to terrorist fundraising. Cryptocurrency also has been used to pay for illegal drugs, firearms, and tools to commit cybercrimes, as well as to facilitate sophisticated ransomware and blackmail schemes.

Buying and selling illegal things. Criminals increasingly use cryptocurrency to purchase and to sell illicit items, such as drugs,⁷ child sexual abuse material,⁸ firearms, explosives, and toxic substances. There is also a robust market for counterfeit identification documents and for unlawfully obtained personal information, such as stolen credit card numbers. As discussed further below, purchases and sales of illegal goods and services using cryptocurrency often take place via dark web marketplaces created explicitly for the purpose of facilitating illicit transactions.⁹

Buying and selling tools to commit crimes or to support terrorism. Criminals and terrorists also use cryptocurrency to buy and sell “tools of the trade”—i.e., items that may or may not themselves be unlawful but are used for subsequent unlawful conduct. Such tools include raw materials to manufacture drugs or explosives, as well as cyber tools and computing capabilities (including servers and domains) to engage in cybercrime or to

conduct malign influence campaigns over social media. Criminals and terrorists have purchased these items and services using cryptocurrency, hoping that their activity and planning would go unnoticed.¹⁰

Ransom, blackmail, and extortion.

Increasingly, criminal extortion schemes are carried out in the digital space. Bad actors can use cryptocurrency as a payment method to facilitate ransom and blackmail without having to demand suitcases full of cash or risk bank accounts being traced. Moreover, criminals routinely infect victims' computers and servers with ransomware, which is a type of malicious software designed to encrypt or otherwise block access to valuable data until the victim agrees to provide a specified payment.¹¹ Criminals also demand payment after threatening to distribute confidential or embarrassing information (such as nude photos in cases of "sextortion") or engaging in "virtual kidnappings" where victims are misled into believing a loved one has been taken.

In April 2020, the Federal Bureau of Investigation ("FBI") issued an advisory about a potential increase in cryptocurrency fraud schemes due to the COVID-19 pandemic. The FBI noted that fraudsters were leveraging the fear and uncertainty caused by the pandemic to carry out scams in new ways. For example, some scammers threatened to infect victims and their families with coronavirus unless they sent payment in bitcoin. Others offered phony or defective products for sale using cryptocurrency with the promise that the products would cure or prevent the disease.¹²

Raising funds for criminal and terrorist activity. Cryptocurrency technology also

has created new ways for criminal enterprises and terrorist organizations to raise funds. For example, as the notorious "Welcome to Video" case reveals, bitcoin has been used to monetize the production of child exploitation material—a development rarely seen before the rise of cryptocurrency. In addition to traditional fundraising, cryptocurrency also provides bad actors and rogue nation states with the means to earn profits directly by mining virtual currency, whether through legitimate mining operations or through illicit "cryptojacking" schemes, which are described further below.¹³

There is also evidence that certain terrorist groups are raising funds using cryptocurrency. While public data on terrorist use of cryptocurrency is limited, it is clear that terrorist networks have conducted fundraising operations through Internet-based crowdsourcing platforms in an attempt to evade stopgaps built into the international banking system.¹⁴ In August 2015, for example, an individual was sentenced to over 11 years in federal prison for conspiring to provide material support and resources to the Islamic State of Iraq and al-Sham ("ISIS"), including by using social media to instruct donors on how bitcoin could provide untraceable financial support to terrorist groups.¹⁵ More recently, in August 2020, the Department of Justice announced the government's largest-ever seizure of cryptocurrency in the terrorism context, stemming from the dismantling of terrorist financing campaigns involving the al-Qassam Brigades (Hamas's military wing), al-Qaeda, and ISIS. Each of those groups had used cryptocurrency technology and social media platforms to spread their influence and raise funds for terror campaigns.¹⁶

SAMSAM

In a high-profile investigation into “21st-century digital blackmail,” a federal grand jury in November 2018 indicted two Iranian men for a 34-month-long international computer hacking and extortion scheme involving the deployment of the sophisticated “SamSam” ransomware.¹⁷ According to the indictment, starting in December 2015, the defendants allegedly accessed victims’ computers, installed the SamSam ransomware, and then ran the program to encrypt critical data. The

defendants demanded ransom paid in bitcoin in exchange for the keys needed to decrypt the victims’ data. The defendants then allegedly exchanged the bitcoin proceeds into Iranian rial using Iran-based entities. All told, the defendants are alleged to have collected over \$6 million in ransom payments and to have caused over \$30 million in losses to more than 200 victims, which included hospitals, municipalities, and public institutions from around the world.



The image is a red and white FBI wanted poster. At the top left is the FBI seal. The text reads: "WANTED BY THE FBI" in large white letters on a red background. Below that, "SAMSAM SUBJECTS" is written in red. The charges are listed in red: "Conspiracy to Commit Fraud and Related Activity in Connection with Computers; Conspiracy to Commit Wire Fraud; Intentional Damage to a Protected Computer; Transmitting a Demand in Relation to Damaging a Protected Computer". Two photos are shown: a man with dark hair and a beard (Mohammad Mehdi Shah Mansouri) and a black silhouette (Faramarz Shahi Savandi). Below the photos are their names. The poster includes sections for "REMARKS", "DETAILS", and contact information for the Newark field office.

WANTED BY THE FBI

SAMSAM SUBJECTS

Conspiracy to Commit Fraud and Related Activity in Connection with Computers; Conspiracy to Commit Wire Fraud; Intentional Damage to a Protected Computer; Transmitting a Demand in Relation to Damaging a Protected Computer

Mohammad Mehdi Shah Mansouri

Faramarz Shahi Savandi

REMARKS

Mohammad Mehdi Shah Mansouri is an Iranian male with a date of birth of September 24, 1991. He has brown hair and brown eyes and was born in Qom, Iran.

Faramarz Shahi Savandi is an Iranian male who was born in Shiraz, Iran, on September 16, 1984. Both men are known to speak Farsi and reside in Tehran, Iran.

DETAILS

Mohammad Mehdi Shah Mansouri and Faramarz Shahi Savandi are wanted for allegedly launching SamSam ransomware, aka MSIL/Samas.A attacks, which encrypted hundreds of computer networks in the United States and other countries. Since December of 2015, Shah Mansouri and Shahi Savandi have received over \$6 million in ransom payments from victims across several sectors, including critical infrastructure, healthcare, transportation, and state/local governments.

On November 26, 2018, a federal grand jury sitting in the United States District Court for the District of New Jersey, Newark, New Jersey, indicted Shah Mansouri and Shahi Savandi on charges of conspiracy to commit fraud and related activity in connection with computers, conspiracy to commit wire fraud, intentional damage to a protected computer, and transmitting a demand in relation to damaging a protected computer. The District of New Jersey issued a federal arrest warrant for both men.

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

Field Office: Newark

www.fbi.gov

Figure 5: The “SamSam” Ransomware Attack – An Example of 21st Century Digital Blackmail

WELCOME TO VIDEO

On October 16, 2019, the Department of Justice announced the indictment and arrest of the alleged operator of Welcome to Video, a darknet child pornography website that was the world's largest online child sexual exploitation market at the time of its seizure. Welcome to Video allegedly offered child sexual exploitation photos and videos for sale using bitcoin, and relied on virtual currency accounts to fund the site and to promote further exploitation of children. The site allegedly hosted approximately eight terabytes of child sexual exploitation material—including over 250,000 unique videos—and claimed over one million downloads of exploitative material by its users. In addition to the operator, at least 337 users of the site have been arrested and charged across the United States and around the world. The globally coordinated law enforcement operation targeting Welcome to Video and its users led to the rescue of at least 23 minor victims who were actively being abused, allegedly by the site's users.¹⁸



Figure 6: Welcome to Video Website after Seizure by the Government

DISMANTLING OF TERRORIST FINANCING CAMPAIGNS

On August 13, 2020, the Department of Justice announced the dismantling of three terrorist financing cyber-enabled campaigns involving the al-Qassam Brigades, al-Qaeda, and ISIS. Investigation revealed that these terrorist groups used sophisticated cyber-tools to assist in financing their operations, including through online solicitation of cryptocurrency donations from supporters around the world. The government has filed three civil forfeiture complaints and a criminal complaint involving the seizure of four websites, four Facebook pages, over 300 cryptocurrency accounts, and millions of dollars.

Al-Qassam Brigades. According to the government’s complaint, the al-Qassam Brigades posted requests for bitcoin donations on its social media page and official websites, claiming that such donations would be untraceable and used to support violent causes. The group’s websites included videos on how to make anonymous donations using unique bitcoin addresses. Fortunately, IRS, HSI, and FBI personnel were able to track and seek forfeiture of the 150 cryptocurrency accounts used to launder funds to and from the al-Qassam Brigades’ accounts.

Al-Qaeda. The government’s investigation also revealed that al-Qaeda and affiliated terrorist groups operated a bitcoin money laundering network using social media platforms and encrypted messaging apps to solicit cryptocurrency donations. In some cases, the groups claimed to be acting as charities, while actually soliciting funds for violent terrorist attacks. Al-Qaeda and their affiliates used sophisticated techniques in an attempt to conceal their fundraising efforts, but law enforcement was able to identify and seek forfeiture of 155 virtual currency assets linked to the groups.

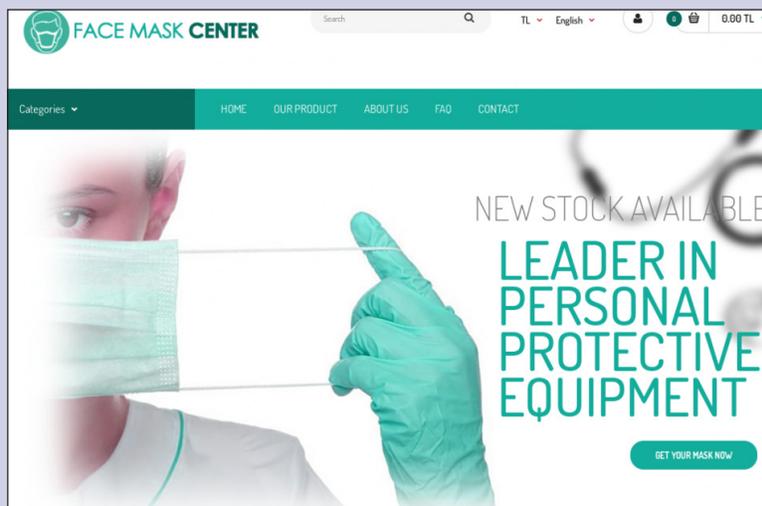
ISIS. Finally, the government’s investigation uncovered a scheme whereby individuals associated with ISIS marketed fake personal protective equipment (“PPE”)—such as N95 respirator masks—to customers across the globe in an effort to take advantage of the COVID-19 pandemic. The funds from such sales would have been used to support ISIS’s operations.²¹

Figure 8: “Donate Anonymously with Cryptocurrency” – An al-Qaeda-Affiliated Group Seeks Anonymous Donations in Bitcoin



The group that posted the request for donations claimed to be a Syrian charity, but allegedly sought funds to support “the mujahidin in Syria with weapons, financial aid and other projects assisting the jihad.”²²

Figure 9: Website Maintained by an ISIS Facilitator to Sell Fake PPE



2. Using Cryptocurrency to Hide Financial Activity

In addition to being used directly in transactions to commit crime or to support terrorism, bad actors also use cryptocurrency to hide and to promote financial activities attendant to unlawful conduct.

Money laundering. Criminals of all types are increasingly using cryptocurrency to launder their illicit proceeds. Broadly speaking, money laundering occurs when an individual knowingly conducts a financial transaction connected to or stemming from a criminal offense in order to promote the

BITCOIN MAVEN

In July 2018, Theresa Tetley, known by her online moniker “Bitcoin Maven,” was sentenced to one year in federal prison for money laundering and for operating an unlicensed bitcoin-for-cash money-transmitting business. Through her unregistered bitcoin exchange business, Tetley facilitated money laundering by providing money-transmission services to members of the public, including at least one individual who received bitcoin from the sale of drugs on the dark web. Tetley also conducted an exchange of bitcoin for cash with an undercover agent who represented that his bitcoin were the proceeds of narcotics trafficking. In sentencing documents, the government revealed that Tetley’s business “fueled a black-market financial system” that “purposely and deliberately existed outside of the regulated bank industry.”²³

offense, conceal the proceeds, or evade federal reporting requirements.²⁴ Such conduct can be substantially easier when the movement of funds takes place online and anonymously, involving the exchange of cryptocurrency for other forms of cryptocurrency or the conversion of cryptocurrency to fiat currency. Indeed, the explosion of online marketplaces and exchanges that use cryptocurrency may provide criminals and terrorists with new opportunities to transfer illicitly obtained money in an effort to cover their financial footprints and to enjoy the benefits of their illegitimate earnings. Transnational criminal organizations, including drug cartels, may find cryptocurrency especially useful to hide financial activities and to move vast sums of money efficiently across borders without detection.

Operating unlicensed, unregistered, or non-compliant exchanges. Criminals may also attempt to hide financial activity by using cryptocurrency exchanges that do not comply with internationally recognized anti-money laundering (“AML”) and combating the financing of terrorism (“CFT”) standards (together, “AML/CFT”).²⁵ In general, “virtual currency exchangers” and “virtual currency exchanges” are, respectively, individuals and entities engaged in the business of exchanging virtual currency for fiat currency, other forms of virtual currency, or other types of assets—and vice versa—typically for a commission.²⁶

Unlicensed or unregistered exchanges or money transmitting businesses can “provide an avenue of laundering for those who use digital currency for illicit purposes.”²⁷ In

BTC-e

In 2017, prosecutors in the United States announced the indictment of the virtual currency exchange “BTC-e” and of one of the exchange’s principal operators. BTC-e received more than \$4 billion worth of bitcoin over the course of its operation. According to the indictment, to appeal to criminals as a customer base, BTC-e did not require users to validate their identities, obscured and anonymized transactions and sources of funds, and lacked appropriate anti-money laundering processes. As a result, the exchange predictably served as a hub for international criminals seeking to hide and launder ill-gotten gains. The indictment alleges that BTC-e facilitated transactions for cybercriminals worldwide and received criminal proceeds from numerous computer intrusions and hacking incidents, ransomware scams, identity theft schemes, corrupt public officials, and narcotics distribution rings. The Department of Justice filed criminal charges, and the Department of the Treasury’s Financial Crimes Enforcement Network (“FinCEN”) assessed a \$110 million civil penalty against the exchange for willfully violating U.S. anti-money laundering laws, and a \$12 million penalty against the exchange’s operator personally.²⁸ BTC-e is only one example in a series of cases in which the Department of Justice has pursued criminal charges against cryptocurrency exchanges for operating as unlicensed money services businesses.²⁹

addition, even properly registered exchanges can serve as a haven for criminal activity by operating under lax rules or by flouting AML protocols. In the normal course, registered exchanges that comply with AML standards and “know your customer” (“KYC”) requirements are likely to possess relevant transactional information. However, exchanges that avoid compliance with such requirements provide criminals and terrorists with opportunities to hide their illicit financial activity from regulators and investigators. Moreover, as discussed in Part II.C below, the requirements for exchanges to register, obtain licenses, and collect information about customers and their transactions are not consistent across international jurisdictions. This inconsistency can create challenges for international law enforcement and regulatory agencies operating in this space.

Evading taxes. As with money laundering, the potential difficulties in tracking cryptocurrency transactions can also facilitate tax evasion. Because of these difficulties, tax cheats may believe that the Internal Revenue Service is not able to uncover or attribute their cryptocurrency transactions, and they may even use additional anonymizing features of cryptocurrencies to further obfuscate their transactions. Tax cheats may then attempt tax evasion by, among other things, not reporting capital gains from the sale or other disposition of their cryptocurrency, not reporting business income received in cryptocurrency, not reporting wages paid in cryptocurrency, or using cryptocurrency to facilitate false invoice schemes designed to fraudulently reduce business income.³⁰ Importantly, the tax loss from unreported capital gains can

be significant as cryptocurrencies emerge and fluctuate in the market. For example, the value of one bitcoin famously rose from around \$1,000 to around \$20,000 in 2017, as investors rushed to that cryptocurrency as an investment vehicle.

Avoiding sanctions. Finally, individuals, companies, and rogue regimes may use cryptocurrency in attempt to avoid the reach of economic sanctions imposed by the United States or other rule-of-law countries. Cryptocurrency’s decentralized and peer-to-peer format may allow sanctioned entities to bypass the financial controls built into traditional financial marketplaces to enforce such sanctions. Indeed, public reports note that several nations have explored the creation and use of their own state-sponsored cryptocurrencies, which could serve as a platform to evade financial controls and oversight. As explained by the U.S. Department of the Treasury, for example, Venezuela attempted to launch a national cryptocurrency—called the “Petromoneda” or “Petro”—in the “hope that the [cryptocurrency] would allow Venezuela to circumvent U.S. financial sanctions.”³¹ Other countries, including Russia and Iran, have threatened to use existing cryptocurrencies to dodge sanctions or to develop their own cryptocurrencies specifically to avoid international oversight.³²

3. Committing Crimes within the Cryptocurrency Marketplace Itself

In addition to offering a means to commit old crimes in new ways, cryptocurrencies and the platforms on which they operate have often

themselves become the target of criminal activity. To protect future victims, as well as to safeguard the integrity of cryptocurrency technology, more must be done to promote security and combat criminal activity on digital exchanges and platforms.

Theft and fraud. Cryptocurrency’s features, as well as the overall “opaqueness and lack of transparency in the cryptocurrency market,”³³ make it particularly attractive, adaptable, and scalable as a target for theft. Criminals—and even rogue state actors³⁴—can steal cryptocurrency by exploiting security vulnerabilities in wallets and exchanges. Thieves can hack wallets and exchanges directly; employ social engineering and other tools to obtain passwords and PINs from unsuspecting users; or, if they themselves operate exchanges, engage in insider theft. Public reports estimate that at least \$1.7 billion of cryptocurrency was stolen or scammed in 2018, with over \$950 million of that amount stolen from cryptocurrency exchanges. In 2019, over \$4.5 billion of cryptocurrency reportedly was lost to theft or fraud, more than doubling the losses from the prior year.³⁵ This susceptibility to theft on a massive scale demonstrates that the lack of appropriate regulation and monitoring of cryptocurrency exchanges poses a threat to cryptocurrency users themselves, as well as to the general public.

In addition to digital theft, fraudsters use cryptocurrency to bilk unsuspecting investors, to promote scams, and to engage in market manipulation. For example, in July 2018, Jon E. Montroll pleaded guilty to securities fraud and to obstruction of

justice related to his operation of two online Bitcoin services: WeExchange Australia, Pty. Ltd., a Bitcoin depository and currency exchange service, and BitFunder.com, which facilitated the purchase and trading of virtual shares of business entities that listed shares on the platform. Montroll pleaded guilty to converting a portion of WeExchange users' bitcoin to his personal use without the users' knowledge or consent. Montroll also admitted failing to disclose a hack of the BitFunder programming code that caused the platform to credit hackers with profits they did not earn, thereby enabling the hackers to wrongfully withdraw approximately 6,000 bitcoin. The hack meant that Montroll lacked the bitcoin necessary to cover what he owed to investors. Despite this, and as a result of his omissions and misrepresentations, Montroll still raised approximately 978 bitcoin after the discovery of the hack. In addition to committing securities fraud, Montroll provided a falsified screenshot and false and misleading answers to Securities and Exchange Commission ("SEC") personnel during the course of their investigation.³⁶

In another fraudulent scheme involving cryptocurrency, Joseph Kim was sentenced in November 2018 to 15 months in federal prison for misappropriating \$1.1 million in bitcoin and litecoin. Kim worked as an assistant trader for a Chicago trading firm that had formed a cryptocurrency group to engage in trading of virtual currencies. Over a two-month period in 2017, Kim misappropriated at least \$600,000 of his trading firm's bitcoin and litecoin cryptocurrency for his own personal benefit, and made false statements and representations

to the company's management to conceal the theft. Subsequently, Kim engaged in another scheme in which he incurred \$545,000 in losses by trading cryptocurrencies using funds that he solicited from friends through lies.³⁷

Cryptojacking. The ability to digitally mine cryptocurrency provides criminals an independent reason to hack into and co-opt computers belonging to unsuspecting individuals and organizations. The unauthorized use of someone else's computer to generate (or "mine") cryptocurrency is called "cryptojacking."³⁸ This is often accomplished through the use of malware or compromised websites, which cause the victim's computer to run crypto-mining code. Considering the value of cryptocurrency compared to the relative ease of secretly using a victim's computer, cryptojacking is another relatively low-risk but high-reward illegal activity made possible by cryptocurrency technology. Reports indicate that rogue states, such as North Korea, have explored using malware to mine cryptocurrency illicitly.³⁹

D. The Role of Darknet Markets

Many of the cryptocurrency-related crimes described above are made possible through the operation of online black markets on the dark web. Indeed, much of the illicit conduct involving cryptocurrency occurs via darknet websites and marketplaces that allow criminals around the world to connect in unregulated virtual bazaars with a great deal of anonymity. These illicit marketplaces offer the opportunity not only to buy and to

OPERATION DISRUPTOR

In September 2020, the Department of Justice joined Europol to announce the results of Operation DisrupTor, a coordinated international effort to disrupt opioid trafficking on the dark web. The extensive operation lasted nine months and was conducted across the United States and Europe, demonstrating international law enforcement's continued partnership against the illegal sale of drugs and other illicit goods and services.

Following the Wall Street Market takedown in May 2019, U.S. and international law enforcement agencies obtained intelligence to identify dark web drug traffickers, resulting in a series of complementary, but separate, law enforcement investigations. Operation DisrupTor actions have resulted in the arrest of 179 dark web drug traffickers and fraudulent criminals who engaged in tens of thousands of sales of illicit goods and services across the United States and Europe.

This operation resulted in the seizure of over \$6.5 million in both cash and virtual currencies; approximately 500 kilograms of drugs worldwide; 274 kilograms of drugs, including fentanyl, oxycodone, hydrocodone, methamphetamine, heroin, cocaine, ecstasy, MDMA, and medicine containing addictive substances in the United States; and 63 firearms.

Operation DisrupTor led to 121 arrests in the United States including two in Canada at the request of the United States, 42 in Germany, eight in the Netherlands, four in the United Kingdom, three in Austria, and one in Sweden. A number of investigations are still ongoing to identify the individuals behind dark web accounts. Operation DisrupTor illustrates the investigative power of federal and international partnerships to combat the borderless nature of online criminal activity, including activity using cryptocurrency.



DEEPPDOTWEB

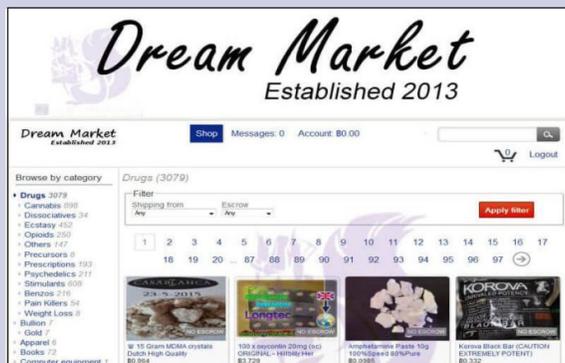
In May 2019, the Department announced the indictment of the alleged owners and operators of the website known as DeepDotWeb (“DDW”) on charges of money laundering conspiracy. According to the indictment, DDW served as a gateway that provided users with access to numerous darknet marketplaces offering for sale illegal narcotics (including fentanyl, heroin, and crystal meth), firearms, malicious software, hacking tools, stolen credit card information, and other contraband. The owners of DDW allegedly received payments—styled as “referral bonuses”—paid in virtual currency to a DDW-controlled bitcoin wallet from individuals who used the site to purchase illicit items. DDW’s owners allegedly attempted to conceal the nature of these illegal payments, which totaled more than \$15 million, by transferring the bitcoin they received to other bitcoin addresses and to bank accounts opened under the names of shell companies. During the course of the conspiracy, DDW’s owners are alleged to have referred hundreds of thousands of users to darknet marketplaces, including AlphaBay, Agora Market, Abraxas Market, Dream Market, Valhalla Market, Hansa Market, TradeRoute Market, Dr. D’s, Wall Street Market, and Tochka Market. In turn, these users completed hundreds of millions of dollars’ worth of allegedly illicit transactions.⁴⁰



Figure 10: Anatomy of the DeepDotWeb Criminal Operation

DREAM MARKET

In October 2018, an administrator of the darknet marketplace Dream Market was sentenced to 20 years in federal prison for narcotics trafficking and money laundering. The defendant, Gal Vallerius, initially participated in the marketplace as a vendor, selling Oxycodone and Ritalin. He later acted as an administrator and senior moderator, supporting



illicit narcotics and money laundering transactions between the site's buyers and vendors. Following the dismantling of Silk Road and

AlphaBay, Dream Market had become one of the largest darknet criminal marketplaces, and all of its items and services were offered for sale in exchange for bitcoin or other peer-to-peer cryptocurrencies.

sell illegal goods and tools for committing crimes, but also to launder money and to hide ill-gotten gains. As a result, darknet markets are a natural place for cryptocurrency to be widely used and exploited.

One of the most notorious online darknet websites, which relied exclusively on bitcoin, was known as Silk Road. Prior to being dismantled by law enforcement in 2013, Silk Road served as an extensive online criminal marketplace used by thousands of drug dealers and other vendors to distribute hundreds of kilograms of illegal drugs and other unlawful goods and services to well over 100,000 buyers. Silk Road was also used to launder hundreds of millions of dollars in illicit proceeds. When the site was

shut down, other cryptocurrency-reliant darknet marketplaces sprung up in its place. Working closely with its international law enforcement partners, the Department of Justice's efforts to dismantle these virtual black markets continue in earnest, including the successful disruption of the notorious AlphaBay and Hansa marketplaces in July 2017; the Wall Street Market ("WSM") and DeepDotWeb ("DDW") websites in May 2019;⁴¹ and the coordinated takedowns of darknet markets dedicated to opioid trafficking reflected in Operation SaboTor (March 2019)⁴² and Operation DisrupTor (September 2020).⁴³ Cryptocurrencies played a central facilitating role in each of these global criminal enterprises. For example, as the Department announced at

the time that indictments were returned against the alleged owners and operators of DDW, “Between in and around November 2014 and April 10, 2019, DDW received approximately 8,155 bitcoin in kickback payments from darknet marketplaces, worth approximately \$8,414,173 when adjusted for the trading value of bitcoin at the time of each transaction.”⁴⁴ Attesting to the complexity of these illicit cross-border payments, many of which took place entirely outside of the established international banking network, the bitcoin was transferred to DDW’s bitcoin wallet, which the defendants are alleged to have controlled, in a series of “more than 40,000 deposits,” and was subsequently withdrawn to various destinations (both known and unknown) around the world through over 2,700 transactions.⁴⁵

II. Law and Regulations

As discussed in Part I, a wide range of criminal activity may involve or be facilitated by the use of cryptocurrency. On numerous occasions, the Department of Justice has used available legal tools to pursue successful prosecutions of such activity. This Part provides an overview of the legal authorities the Department uses to prosecute those who misuse cryptocurrency, and describes the roles and responsibilities of the Department’s key government partners.

A. Criminal Code Authorities

As discussed above, cryptocurrency is often the preferred payment method for the distribution of contraband and of other illegal goods and services, and it can be used

to collect funds from victims of traditional fraud or computer intrusions. A wide variety of federal charges can be brought to bear for such conduct, including, for example:

- **Wire fraud**, 18 U.S.C. § 1343. (For examples of cryptocurrency prosecutions involving the wire fraud statute, see the indictment of AriseBank CEO Jared Rice, Sr., discussed on pages 31-32, and the indictment of two Iranian men for deployment of SamSam ransomware, discussed on pages 8 and 26.)
- **Mail fraud**, 18 U.S.C. § 1341.
- **Securities fraud**, 15 U.S.C. §§ 78j and 78ff. (For example, see the indictment of AriseBank CEO Jared Rice, Sr., discussed on pages 31-32, and the indictment of Jon E. Montroll, discussed on pages 15-16.)
- **Access device fraud**, 18 U.S.C. § 1029. (For example, see the indictment of AlphaBay, discussed on pages 19 and 47.)
- **Identity theft and fraud**, 18 U.S.C. § 1028. (For example, see the indictment of AlphaBay, discussed on pages 19 and 47.)
- **Fraud and intrusions in connection with computers**, 18 U.S.C. § 1030. (For example, see the indictment of two Iranian men for deployment of SamSam ransomware, discussed on pages 8 and 26.)
- **Illegal sale and possession of firearms**, 18 U.S.C. § 921 *et seq.*
- **Possession and distribution of counterfeit items**, 18 U.S.C. § 2320.

- **Child exploitation activities**, 18 U.S.C. § 2251 *et seq.* (For example, see the indictment of Ammar Atef Alahdali, discussed on page 6, footnote 8.)

- **Possession and distribution of controlled substances**, 21 U.S.C. § 841 *et seq.* (For example, see the indictment of AlphaBay, discussed on pages 19 and 47.)

The Department also can bring to bear a wide variety of money laundering charges in cases involving misuse of cryptocurrency. Depending on the facts and circumstances, transactions involving cryptocurrency can form the basis of concealment, promotion, sting, and international money laundering violations. In addition, individuals and companies engaged in money transmission involving virtual assets, referred to below as “virtual asset service providers,” may be subject to, and may fail to comply with, both federal and State registration, record keeping, and reporting requirements. Potential charges include, for example:

- **Money laundering**, 18 U.S.C. § 1956 *et seq.* (For examples of cryptocurrency prosecutions involving the federal money laundering statute, see the indictment of BTC-e and its operator, discussed on pages 14 and 46; the indictment of AlphaBay, discussed on pages 19 and 47; the indictment of a Dutch national for his operation of DarkScandals, discussed on page 10; and the indictment of two Chinese nationals, discussed on pages 27-28.)

- **Transactions involving proceeds of illegal activity**, 18 U.S.C. § 1957. (For example, see the indictment of BTC-e and its operator, discussed on pages 14 and 46.)

- **Operation of an unlicensed money transmitting business**, 18 U.S.C. § 1960 (For example, see the indictment of BTC-e and its operator, discussed on pages 14 and 46, and the indictment of two Chinese nationals, discussed on pages 27-28.)

- **Failure to comply with Bank Secrecy Act requirements**, 31 U.S.C. § 5331 *et seq.*

Virtual asset transactions may also form the basis for prosecution if, for example, they are used as a means to provide material support or resources to terrorists or foreign terrorist organizations.⁴⁶ Such transactions could also be used for payments that facilitate other crimes implicating national security, such as espionage⁴⁷ or conspiracies involving interference in the political process, in violation of various federal laws.

Finally, the Department frequently uses existing criminal authorities to seize and forfeit virtual assets and other property derived from or involved in activity of an individual or organization charged with a crime. The Department also uses available civil authorities for such seizures and forfeitures, which allow the government to “arrest” the assets themselves, even in cases where no person is charged criminally or where a defendant may not be prosecutable due to, for example, death or flight from a jurisdiction. Statutory authorities for forfeiture include:

- **Criminal forfeiture**, 18 U.S.C. § 982; 21 U.S.C. § 853. (For examples of cryptocurrency prosecutions involving the criminal forfeiture statute, see the indictment

of the alleged administrator of Helix, discussed on page 43, and the indictment of two Chinese nationals, discussed on pages 27-28.)

- **Civil forfeiture**, 18 U.S.C. § 981. (For example, see the verified complaints in the AlphaBay case, discussed on pages 9 and 47; the Welcome to Video case, discussed on pages 7 and 9; the DarkScandals case, discussed on page 10; the cases involving the al-Qassam Brigades, al-Qaeda, and ISIS, discussed on pages 7 and 11-12; and the cases involving hacks of virtual currency exchanges by North Korean actors, discussed on pages 27 and 28.)

B. Regulatory Authorities

As described above, the Department of Justice has broad and diverse federal jurisdiction over criminal and other improper conduct that may involve cryptocurrency and other types of virtual assets. A number of regulatory agencies in the United States also have authority to enforce statutes and regulations that apply to various virtual-asset-related activities. The Department has worked closely and cooperatively with these agencies in identifying and proceeding against individuals who misuse cryptocurrency for illicit purposes.

Much of the regulatory activity conducted by the agencies discussed below focuses on money services businesses (“MSBs”) and virtual asset service providers (“VASPs”). In general, MSBs are individuals or entities in one or more of the following capacities:

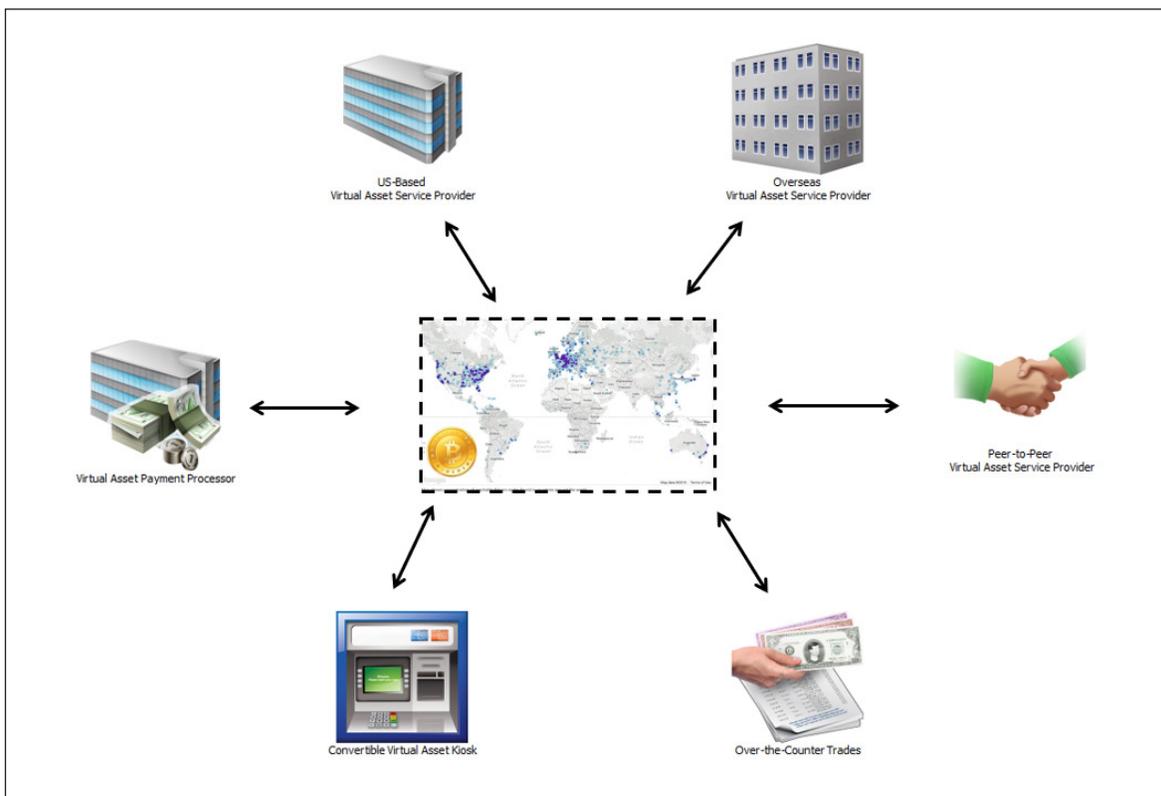
- i. currency dealer or exchanger;
- ii. check casher;
- iii. issuer of traveler’s checks, money orders, or stored value;
- iv. seller or redeemer of traveler’s checks, money orders, or stored value;
- v. money transmitter; or
- vi. the U.S. Postal Service.⁴⁸

VASPs are individuals or entities operating as a business to conduct one or more of the following activities for or on behalf of another entity or individual:

- i. exchanges between virtual assets and fiat currencies;
- ii. exchanges between one or more forms of virtual assets;
- iii. transfers of virtual assets;
- iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; or
- v. participation in and provision of financial services related to an issuer’s offer and/or sale of a virtual asset.⁴⁹

In the United States, individuals and entities that offer money transmitting services involving virtual assets, such as cryptocurrency exchanges and kiosks, as well as certain issuers, exchangers, and brokers of virtual assets, are considered MSBs. Like brick-and-mortar financial institutions, MSBs are subject to AML/CFT⁵⁰ regulations as well as certain licensing and registration requirements, as discussed below.

Figure 11: Depiction of the Operation of a Global Virtual Asset Network



1. The Financial Crimes Enforcement Network and the Bank Secrecy Act

Regulatory authority. MSBs, including cryptocurrency exchanges, function as regulated businesses subject to the federal Bank Secrecy Act (“BSA”).⁵¹ The U.S. Department of the Treasury’s Financial Crimes Enforcement Network (“FinCEN”)

has primary responsibility for administering the BSA and for implementing its regulations.⁵² Part of that responsibility includes maintaining the BSA database, which is a repository of reports about financial transactions that are potentially indicative of money laundering.⁵³ FinCEN serves as the Financial Intelligence Unit (“FIU”) for the United States, meaning it is the central entity responsible for receiving and analyzing suspicious transaction reports and other information concerning money laundering, financing of terrorism, and related offenses.⁵⁴ FinCEN regulates individuals and entities engaged in the business of accepting and transmitting convertible virtual currency (“CVC”), which refers to “virtual currency

that either has an equivalent value as currency, or acts as a substitute for currency, and is therefore a type of ‘value that substitutes for currency.’”⁵⁵ In 2011, FinCEN issued a final rule that, among other things, defined “money transmission services” to include accepting and transmitting “currency, funds, or *other value that substitutes for currency* by any means.”⁵⁶ The phrase “other value that substitutes for currency” was intended to cover situations where a transmission includes something that the parties recognize has value that is equivalent to, or can substitute for, fiat currency.⁵⁷ The definition of “money transmission” is technology-neutral: whatever the platform, protocol, or mechanism, the acceptance and transmission of value from one person to another, or from one location to another, is regulated under the BSA.

To provide additional clarity and to respond to questions from the private sector, FinCEN issued interpretive guidance in March 2013 and in May 2019 regarding the application of its regulations to certain transactions involving the acceptance of currency or funds and the transmission of virtual currency.⁵⁸ The 2013 FinCEN guidance identified the participants in some virtual currency arrangements, including “exchangers,” “administrators,” and “users,” and clarified that while exchangers and administrators generally qualify as money transmitters under the BSA, users do not.⁵⁹ The guidance also stated that virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered MSBs to the extent they accept

and transmit CVC or when they buy or sell CVC for any reason.⁶⁰ As MSBs, such virtual currency administrators and exchangers are obliged to have AML programs, to file Suspicious Activity Reports (“SARs”), and to follow other BSA requirements.⁶¹

The May 2019 FinCEN guidance addressed how FinCEN regulations relating to MSBs apply to various business models involving money transmission denominated in CVC, including with reference to prior administrative rulings.⁶² Importantly, the guidance discussed the application of the BSA to foreign-located MSBs, individual peer-to-peer exchangers, wallet providers, cryptocurrency kiosk operators, CVC-to-CVC transactions, payment processors, mixers and tumblers, initial coin offerings, Internet casinos, trading platforms, decentralized exchanges and distributed applications (“DApps”), miners, software providers, and developers of such technologies. In particular, the guidance outlined the application of FinCEN’s regulations to persons who provide anonymizing services or who are engaged in activities involving anonymity-enhanced CVCs. According to FinCEN, anonymizing service providers and some AEC issuers are money transmitters, whereas an individual or entity that merely provides anonymizing software is not.

FinCEN has stated that MSBs that conduct money transmission in CVCs must meet the same AML/CFT standards as other MSBs under the Bank Secrecy Act. This includes registering with FinCEN, establishing an AML program reasonably designed to prevent

money laundering and terrorist financing, and meeting certain record keeping and reporting obligations, such as filing SARs.⁶³ SARs and currency transaction reports (“CTRs”) are a vital source of information that all MSBs—including VASPs, when applicable—should be generating where appropriate, and filing with FinCEN. These reports may contain leads for law enforcement and information necessary to deter, investigate, and prosecute criminal activity.

Importantly, FinCEN’s requirements apply equally to domestic and foreign-located MSBs—even if the foreign-located MSB does not have a physical presence in the United States.⁶⁴ The MSB need only do business in whole or substantial part in the United States. In addition, parties become money transmitters, and therefore MSBs, whether they exchange from fiat to convertible virtual currency or from one virtual currency to another virtual currency.⁶⁵

Interaction with the Department of Justice. FinCEN’s relationship with the Department of Justice and other law enforcement agencies generally falls into two categories: crime prevention (through compliance requirements that prevent money laundering and terrorist activity) and investigatory assistance (through, for example, the provision of leads for criminal investigations generated by regulatory reporting requirements regarding suspicious activity). In addition, FinCEN has the ability to share and to receive financial intelligence information among foreign counterparts, thus creating an important

international network. FinCEN also has civil enforcement authority through which it can impose monetary penalties to supplement, or as an alternative to, criminal prosecution in appropriate circumstances, and can take regulatory action to address money laundering and terror financing concerns raised in the virtual currency space.⁶⁶

In just one example of successful collaboration, FinCEN, working in coordination with the United States Attorney’s Office for the Northern District of California, assessed a \$700,000 civil monetary penalty in 2015 against Ripple Labs Inc. and its wholly-owned subsidiary, XRP II, LLC.⁶⁷ Ripple Labs, which is headquartered in San Francisco, facilitated transfers of virtual assets and provided virtual asset exchange transaction services. The company also operated a virtual currency known as XRP that, in 2015, was the second-largest cryptocurrency by market capitalization after Bitcoin. Parallel investigations by the Department of Justice and FinCEN found that Ripple Labs willfully violated several requirements of the BSA by acting as an MSB and selling XRP without registering with FinCEN and by failing to implement and maintain an adequate AML program. Ripple Labs entered into a settlement agreement that resolved possible criminal charges and required the entity to forfeit \$450,000. These funds were credited to partially satisfy the \$700,000 civil money penalty. In addition, the settlement agreement required Ripple Labs to engage in steps to ensure future compliance with AML/CFT obligations.⁶⁸



2. Office of Foreign Assets Control

Regulatory authority. Virtual assets move globally, and in some instances they move to entities or jurisdictions subject to economic sanctions administered by the U.S. Department of the Treasury. The Treasury Department’s Office of Foreign Assets Control (“OFAC”) administers and enforces economic and trade sanctions against targeted foreign countries and regimes; terrorist groups; international narcotics traffickers; those engaged in activities related to the proliferation of weapons of mass destruction; those engaged in malicious cyber activities; and other entities that present threats to the national security, foreign policy, or economy of the United States based on U.S. foreign policy and national security goals.⁶⁹

As a general matter, U.S. persons and persons otherwise subject to OFAC jurisdiction—including firms that facilitate or engage in online commerce or process transactions using digital currency⁷⁰—are responsible for ensuring that they do not engage in transactions prohibited by OFAC sanctions (such as dealings with blocked persons or property) or in otherwise-prohibited trade or investment-related transactions.⁷¹ Prohibited transactions generally also include those that evade or avoid, have the purpose of evading or avoiding, cause a violation of, or attempt to violate prohibitions imposed by OFAC under

various sanctions authorities.⁷² In addition, persons who provide financial, material, or technological support for or to a designated person or entity, or certain malicious activities, may themselves be designated by OFAC under the relevant sanctions authority, or be criminally or civilly liable for violations of the Trading With the Enemies Act, the International Emergency Economic Powers Act, and other statutes.⁷³

Interaction with the Department of Justice.

On November 28, 2018, OFAC took its first virtual-asset-related action pursuant to the “cyber sanctions” authorized by Executive Order (“EO”) 13694, as amended by EO 13757.⁷⁴ This action targeted two Iran based individuals who helped exchange bitcoin ransom payments into Iranian rial on behalf of malicious Iranian cyber actors involved with the SamSam ransomware scheme described above.⁷⁵ OFAC also identified two bitcoin addresses associated with these individuals that were connected to over 7,000 transactions worth millions of dollars.⁷⁶ By designating these malicious cyber actors, OFAC sought to “aggressively pursue Iran and other rogue regimes attempting to exploit digital currencies and weaknesses in cyber and AML/CFT safeguards,” while also encouraging “virtual currency exchanges, peer-to-peer exchangers, and other providers of digital currency services [to] harden their networks against [such] illicit schemes.”⁷⁷ As described above, in a related move, the Department of Justice brought criminal charges against the two Iran-based individuals related to the 34-month-long international computer hacking and extortion scheme involving the use of SamSam ransomware against numerous U.S. computer networks.⁷⁸

In August 2019, OFAC designated three Chinese nationals, one Chinese drug trafficking organization, and one Chinese pharmaceutical company for their involvement with fentanyl manufacturing and trafficking pursuant to the Foreign Narcotics Kingpin Designation Act (“Kingpin Act”). OFAC identified cryptocurrency addresses associated with two drug traffickers to maximize disruption of their financial dealings.⁷⁹ OFAC closely coordinated these designations with the Department of Justice. Previously, in 2017, the Department of Justice indicted one of the Chinese nationals for his role as a manufacturer and distributor of fentanyl and other opiate substances.⁸⁰ And in August 2018, the Department of Justice charged two of the Chinese nationals with operating a conspiracy that manufactured and shipped deadly fentanyl analogues and 250 other drugs to at least 25 countries and 37 states.⁸¹

In September 2020, OFAC designated three Russian nationals for having acted or purported to act for or on behalf of, directly or indirectly, the Internet Research Agency (“IRA”), an entity previously designated for its involvement with election interference activities, pursuant to EO 13694, as amended by EO 13757, and EO 13848. The IRA uses cryptocurrency to fund activities in furtherance of ongoing malign influence operations around the world. OFAC identified digital currency addresses for two of these Russian nationals.⁸² Concurrently, the Department of Justice filed a criminal complaint charging one of the Russian nationals for his alleged role in a conspiracy to use the stolen identities of real U.S. persons

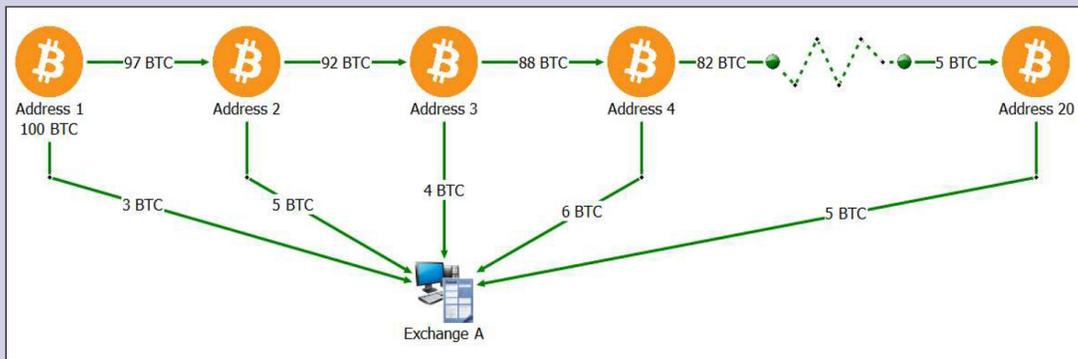
to open fraudulent accounts at banking and cryptocurrency exchanges.⁸³

Earlier, on March 2, 2020, OFAC announced sanctions pursuant to EOs 13722 and 13694, as amended, against two Chinese nationals who are alleged to have laundered over \$100 million worth of cryptocurrency stolen from cryptocurrency exchanges by North Korean actors. This theft is another example of North Korea’s cyber heist program (see page 28), which trains actors to target and launder stolen funds—including large amounts of cryptocurrency—from financial institutions.⁸⁴ The two sanctioned individuals allegedly received the stolen cryptocurrency from accounts controlled by North Korean actors and subsequently transferred the funds among cryptocurrency addresses to obfuscate their origin. As a result of OFAC’s action, “all property and interests in property of these individuals that are in the United States or in the possession or control of U.S. persons must be blocked and reported to OFAC.”⁸⁵ On the same day that OFAC announced these sanctions, the Department of Justice announced criminal charges against the two individuals for money laundering conspiracy and for operating an unlicensed money transmitting business, as well as the seizure of the illicit funds.⁸⁶ Subsequently, on August 27, 2020, the Department filed a complaint seeking civil forfeiture of 280 additional virtual currency addresses and accounts linked to the hacks.⁸⁷ The coordinated actions by OFAC and the Department of Justice followed a comprehensive investigation led by the FBI, IRS–Criminal Investigation, and Homeland Security Investigations, further demonstrating the importance of cooperation among investigatory agencies.

CASE STUDY: THE NORTH KOREAN HACKS

As discussed in the text, on the same day in March 2020 that OFAC announced sanctions, the Department of Justice announced criminal charges against two Chinese nationals for laundering over \$100 million worth of cryptocurrency that the defendants allegedly obtained from North Korean actors who had hacked cryptocurrency exchanges.⁸⁸ In March and August 2020, the Department also announced complaints seeing the civil forfeiture of hundreds of virtual currency accounts associated with related North Korean hacks and subsequent money laundering conspiracies.⁸⁹ The investigations into these criminal schemes revealed highly sophisticated money-laundering techniques. For example, criminal actors allegedly laundered the funds illicitly obtained from the hacks through several intermediary addresses and other virtual currency exchanges. On several occasions, the actors allegedly used the chain-hopping technique in an attempt to obfuscate the transaction path by converting the stolen cryptocurrency into BTC, Tether, or other forms of cryptocurrency.⁹⁰ The actors also allegedly used “peel chains” to conceal their activity, whereby “a large amount of [cryptocurrency] sitting at one address is sent through a series of transactions in which a slightly smaller amount of [cryptocurrency] is transferred to a new address each time.”⁹¹

Figure 12: Depiction of a Simple “Peel Chain”



This chart depicts a hypothetical “peel chain” where a subject deposits 100 total bitcoin into an exchange. The subject forwards the bitcoin through a series of 20 “peels” in inconsistent amounts in an attempt to make the underlying transaction difficult to track. In practice, sophisticated cybercriminals often use hundreds of transactions to obscure the path of funds.⁹²

The successful investigations into the North Korean cryptocurrency hacks and subsequent money-laundering scheme—and the coordinated actions between OFAC and the Department of Justice—demonstrate the importance of interagency coordination in addressing threats within the virtual currency space.



3. Office of the Comptroller of the Currency

The Office of the Comptroller of the Currency (“OCC”) is an independent branch of the U.S. Department of the Treasury that charters, regulates, and supervises national banks and federal savings associations. OCC issues rules and regulations for banks and can “impos[e] corrective measures, when necessary, on OCC-governed banks that do not comply with laws and regulations or that otherwise engage in unsafe or unsound practices.”⁹³ On July 22, 2020, OCC published an Interpretive Letter to clarify the authority of national banks and federal savings associations to provide cryptocurrency custody services for their customers.⁹⁴ The Letter concludes that such services, which include “holding the unique cryptographic keys associated with cryptocurrency,” are a permissible modern form of traditional bank activities.⁹⁵ It also stressed OCC’s position that banks can provide their services to lawful cryptocurrency businesses “so long as they effectively manage the risks and comply with applicable law.”⁹⁶

Earlier in 2020, OCC entered into a cease-and-desist consent order with M.Y. Safra Bank, after alleging that the bank violated the BSA’s requirements for establishing an adequate AML program and failed to

investigate suspicious transactions and to timely file SARs. Among other things, OCC’s investigation revealed that the bank failed to sufficiently consider AML risks and implement appropriate risk controls when opening accounts for customers that operated virtual-currency money services businesses.⁹⁷ Pursuant to the consent order, the bank must adopt numerous improvements to its risk profile, system of internal controls, customer due diligence operation, and BSA audit program.



4. The Securities and Exchange Commission

Regulatory authority. The mission of the U.S. Securities and Exchange Commission (“SEC”) is to protect investors; to maintain fair, orderly, and efficient markets; and to facilitate capital formation. Of particular relevance to the SEC’s mission in the virtual currency context is the rapid growth of the “initial coin offerings” (“ICOs”) market and its widespread promotion as a means for new investment opportunity, which has provided fertile ground for malicious actors to swindle investors. ICOs (which are also known as “token sales”⁹⁸) are a means companies have used to raise capital by offering and selling digital tokens to potential investors in exchange for funding a certain project or platform. The tokens purchased by an investor in an ICO, which are distributed

via a blockchain network, typically do not provide traditional “shares” in the issuing company. Instead, they might purport to grant access to a good or service, to the right to a share in the relevant project’s earnings, or to a potential increase in value based on the project’s success.⁹⁹ Recognizing the securities law implications for technological developments like blockchain and distributed ledger technologies, digital assets (including cryptocurrency), digital asset securities, and other digital instruments, the SEC has devoted substantial resources to this area.¹⁰⁰

In 2017, the SEC issued an investigative report cautioning the public that offers and sales of digital assets—including through ICOs and token sales—by “virtual” organizations may be subject to the requirements of the federal securities laws, which include registration and disclosure mandates.¹⁰¹ As the SEC explained, “[w]hether or not a particular transaction involves the offer or sale of a security—regardless of the terminology or technology used—will depend on the facts and circumstances, including the economic realities of the transaction.”¹⁰² To protect investors and the public, the SEC has summarily suspended, for 10 business days, the trading of securities of more than a dozen issuers when there were concerns about the accuracy and adequacy of information in the marketplace regarding securities offered or sold through ICOs or coin- or token- related news.¹⁰³ The SEC also has warned investors about potential scams involving companies claiming to be related to, or asserting they are engaging in, ICOs. And the SEC has filed ICO-related civil enforcement actions against individuals violating the securities laws or engaging in fraudulent schemes.¹⁰⁴

On April 3, 2019, the SEC Staff released a framework for analyzing whether “a digital asset is offered or sold as an investment contract, and, therefore, is a security” under the federal securities laws.¹⁰⁵ The term “security” includes an “investment contract,” as well as other instruments such as stocks, bonds, and transferable shares. Under the so-called “Howey test,” derived from the Supreme Court’s seminal 1946 decision in *Securities and Exchange Commission v. W. J. Howey Co.*, an “investment contract” exists if there is an investment of money in a common enterprise with an expectation of profits derived from the efforts of others.¹⁰⁶ The framework is careful to note that, in the digital asset context, as with all other assets, this analysis does not depend only on the “form and terms” of the asset itself, “but also on the circumstances surrounding the digital asset and the manner in which it is offered, sold, or resold.”¹⁰⁷ The SEC encourages individuals and entities in the digital asset marketplace to engage proactively with SEC staff as the marketplace continues to develop.¹⁰⁸

A high-profile action brought by the SEC in October 2019 highlights the need for individuals and entities in the global digital asset marketplace to ensure they are in compliance with U.S. federal securities laws. That month, the SEC sought and received a temporary restraining order against two offshore entities conducting an unregistered, ongoing digital token offering both within the United States and overseas that had raised more than \$1.7 billion of investor funds.¹⁰⁹ According to the SEC’s complaint, “Telegram Group Inc. and its wholly-owned subsidiary

TON Issuer Inc. began raising capital in January 2018 to finance the companies' business, including the development of their own blockchain, the 'Telegram Open Network' or 'TON Blockchain,' as well as the mobile messaging application Telegram Messenger."¹¹⁰ As part of their plan to raise funds, the entities sold "approximately 2.9 billion digital tokens called 'Grams' at discounted prices to 171 initial purchasers worldwide, including more than 1 billion Grams to 39 U.S. purchasers."¹¹¹ The SEC's complaint alleged that Telegram and TON Issuer failed to register their offers and sales of the new "Grams" cryptocurrency, in violation of the registration provisions of the Securities Act of 1933.¹¹²

In March 2020, a federal judge granted the SEC a preliminary injunction, ruling that the agency had shown "a substantial likelihood of success in proving that the contracts and understandings at issue, including the sale of 2.9 billion Grams to 175 purchasers in exchange for \$1.7 billion, are part of a larger scheme to distribute those Grams into a secondary public market, which would be supported by Telegram's ongoing efforts."¹¹³ Accordingly, the court concluded that, on the facts before it, "the resale of Grams into the secondary public market would be an integral part of the sale of securities without a required registration statement."¹¹⁴ Three months later, the court approved a settlement between the parties, whereby Telegram and its subsidiary agreed not to appeal the court's ruling and consented to the court's judgment without admitting or denying the SEC's allegations. The court ordered Telegram to disgorge \$1,224,000,000 in ill-gotten gains

from the sale of Grams, with credit for the amounts paid back to initial purchasers of Grams, and also ordered Telegram to pay a civil penalty of \$18,500,000.¹¹⁵

The SEC's landmark Telegram case underscores why companies and individuals working and innovating in the digital assets space should ensure—prior to offering or selling—that their activities will meet all applicable requirements under the federal securities laws.¹¹⁶ Of course, in cases involving outright fraud, bad actors face not only a variety of potential civil securities law violations, but also potential criminal prosecution for fraud or theft.¹¹⁷

Interaction with the Department of Justice. The SEC works closely with the Department of Justice in cases involving criminal violations of the federal securities laws, including cases related to ICOs. As just one example, on January 25, 2018, the SEC filed a civil complaint in federal court in Texas seeking to halt an allegedly fraudulent ICO by AriseBank. The same week, the FBI and the SEC coordinated the timing of a search at the temporary residence of the ICO issuer with the execution of a freeze order by a receiver in the SEC's civil action, resulting in the recovery of cryptocurrency for the victim investors.¹¹⁸ Subsequently, in the Department of Justice's related criminal case, a federal grand jury in Dallas charged AriseBank CEO Jared Rice, Sr., on November 20, 2018, for defrauding investors out of \$4 million worth of cryptocurrency assets. The Department's investigation revealed that Rice claimed in connection with the ICO that a cryptocurrency token called "AriseCoin"

could offer consumers FDIC insured accounts and traditional banking services, in addition to cryptocurrency services. These statements were false. Rice, who had converted investor funds for his own personal use, also claimed falsely that the ICO had raised \$600 million in a matter of weeks.¹¹⁹ On March 20, 2019, Rice pleaded guilty in the criminal proceedings to one count of securities fraud, in violation of 15 U.S.C. §§ 78j and 78ff. In the SEC’s civil action, Rice and AriseBank COO Stanley Ford agreed to pay nearly \$2.7 million in disgorgements, interest, and penalties, without admitting or denying the allegations. Both Rice and Ford are permanently enjoined from violating the antifraud and registration provisions of the federal securities laws, from ever serving as officers or directors of public companies, and from participating in issuances, offers, or sales of digital securities.¹²⁰



5. The Commodity Futures Trading Commission

Statutory authority. Like the SEC, the Commodity Futures Trading Commission (“CFTC”) has statutory authority with respect to certain aspects and uses of virtual assets. Under the Commodity Exchange Act (“CEA”),¹²¹ the CFTC has oversight over derivatives contracts, including futures, options, and swaps,¹²² that involve a

commodity. The CEA defines “commodity” to include agricultural products, “all other goods and articles,” and “all services, rights, and interests . . . in which contracts for future delivery are presently or in the future dealt in.”¹²³ The CFTC has concluded that certain virtual currencies are “commodities” under the CEA.¹²⁴ In addition, multiple federal courts have held that virtual currencies fall within the CEA’s definition of commodity.¹²⁵

The CFTC’s jurisdiction is implicated when a virtual currency is the underlying asset in a derivatives contract, or if there is fraud or manipulation involving a virtual currency traded in interstate commerce. “Beyond instances of fraud or manipulation, the CFTC generally does not oversee ‘spot’ or cash market exchanges and transactions involving virtual currencies which do not utilize margin, leverage, or financing.”¹²⁶ The CFTC has taken action against unregistered bitcoin futures exchanges and firms illegally offering margined or financed retail virtual currency transactions;¹²⁷ enforced laws prohibiting fictitious trades on a derivatives platform¹²⁸ and laws requiring firms to implement adequate anti-money laundering procedures;¹²⁹ issued interpretative guidance concerning whether “actual delivery” has occurred in the context of retail commodity transactions in virtual currencies;¹³⁰ issued warnings about valuations and volatility in spot virtual currency markets;¹³¹ and addressed numerous virtual currency Ponzi schemes.¹³²

Interaction with the Department of Justice. In a case involving parallel action by the Department of Justice, the CFTC on April

16, 2018, filed a complaint in federal court in New York charging Blake Harrison Kantor and Nathan Mullins, as well as several entities located in the United States and abroad, with operating a fraudulent scheme covering binary options and a virtual currency known as ATM Coin.¹³³ The CFTC’s complaint alleged that, since at least April 2014, the defendants solicited potential customers through emails, phone calls, and a website to purchase illegal off-exchange binary options. Additionally, the defendants falsely claimed that customers’ accounts would generate significant profits based upon Kantor’s purported profitable trading history, and allegedly misappropriated a substantial amount of the customer funds for personal use. The defendants were alleged to have sought to cover up their misappropriation by inviting customers to transfer their binary options account balances into ATM Coin. Some customers agreed to transfer their funds into ATM Coin, and at least one customer sent additional money to the defendants to purchase additional ATM Coin. The defendants then allegedly misrepresented to customers that their ATM Coin holdings were worth substantial sums of money. On October 23, 2019, a federal court entered an order finding that the defendants had committed fraud and had misappropriated client funds, and requiring them to pay a total of \$4.25 million.¹³⁴ In a parallel action, the United States Attorney for the Eastern District of New York filed a criminal indictment charging Kantor with fraud, obstruction, and making false statements. He pleaded guilty to the wire fraud conspiracy and obstruction charges, and was sentenced on July 1, 2019, to 86 months’ imprisonment.¹³⁵



6. The IRS and Tax Enforcement

The Internal Revenue Service (“IRS”) treats virtual currency as property for U.S. federal tax purposes, which means that the general tax principles that apply to property transactions also apply to virtual currency transactions.¹³⁶ Income, including capital gains, from virtual currency transactions is taxable, and virtual currency transactions themselves must be reported on a taxpayer’s income tax return.¹³⁷

In addition, wages paid in virtual currency to employees are taxable, reportable on a Form W-2, and subject to withholding and payroll taxes. Businesses that receive payments for goods or services in virtual currency are required to include such payments in their gross income. The Department of Justice’s Tax Division and U.S. Attorney’s Offices around the country may pursue tax related prosecutions in cases involving the failure to report income from virtual currency. The Department of Justice also works with the IRS to support its enforcement and compliance efforts relating to virtual currency, including enforcing summonses issued to taxpayers and third parties, as well as assisting in “John Doe” summons matters.¹³⁸

On October 9, 2019, the IRS issued additional guidance and FAQs for taxpayers who engage in virtual currency transactions, in an effort to help them better understand their reporting obligations. The guidance addresses the tax treatment of “hard forks,” which occur when a cryptocurrency undergoes a protocol change resulting in a new distributed ledger and a new cryptocurrency, in addition to the original distributed ledger.¹³⁹ The FAQs also address more basic questions about, for example, calculating gains or losses when selling or exchanging virtual currency for real currency or property; whether virtual currency paid by an employer for services constitutes taxable income; and maintaining records of transactions in virtual currency.¹⁴⁰ On December 31, 2019, the IRS issued additional FAQs for taxpayers relating to charitable donations in virtual currency.¹⁴¹

7. State Authorities

State attorneys general, securities regulators, and departments of financial services are responsible for protecting the investing public in their respective States by, for example, licensing securities firms and investment professionals (such as broker-dealers and investment advisers); registering certain securities offerings; reviewing financial offerings by companies; auditing sales practices and record keeping; promoting investor education; and enforcing State securities and banking laws.¹⁴² Many State authorities are actively monitoring, supervising, or investigating virtual asset activities within their jurisdictions,

particularly those involving the issuance or sale of ICOs and other investment products.

For example, on May 21, 2018, the North American Securities Administrators Association (“NASAA”)¹⁴³ announced a coordinated series of enforcement actions by State and provincial securities regulators in the United States and Canada to crack down on fraudulent ICOs and cryptocurrency-related investment products, as well as on the fraudsters behind them. More than 40 jurisdictions throughout North America participated in “Operation Cryptosweep,” which resulted in nearly 70 inquiries and investigations and 35 pending or completed enforcement actions related to ICOs or cryptocurrencies.¹⁴⁴

The State of New York has been one of the more proactive States seeking to regulate and gather information in the virtual asset and ICO space. New York State officials are conducting a Virtual Markets Integrity Initiative, which is a fact-finding inquiry into the policies and practices of platforms used by consumers to trade cryptocurrencies.¹⁴⁵ As part of that initiative, on April 17, 2018, the New York Attorney General’s Office sent letters to thirteen entities identified as “major virtual currency trading platforms” or “exchanges,” requesting disclosures about their operations, use of bots, conflicts of interest, outages, and other issues.¹⁴⁶ The letters also requested information on the covered entities’ operations, internal controls, and safeguards to protect customer assets as part of a broader effort to protect cryptocurrency investors and consumers.

C. International Regulation

As discussed further below, the lack of consistent international regulation and enforcement of anti-money laundering and combating the financing of terrorism standards applicable to virtual asset entities represents a major challenge. There are, however, important organizations in the international regulatory space, especially the global standard-setter for AML/CFT standards—the Financial Action Task Force (“FATF”).¹⁴⁷



The Financial Action Task Force. The FATF is an intergovernmental organization that was founded in 1989 on the initiative of the G7 by the ministers of its member jurisdictions.¹⁴⁸ Its objectives are to set standards and to promote effective implementation of legal, regulatory, and operational measures for combating money laundering, terrorist financing, proliferation of weapons of mass destruction, and other related threats to the integrity of the international financial system. As a standard-setting and policy-making body, the FATF works to generate the technical understanding and necessary political will to bring about national legislative and regulatory reforms, which are intended to be harmonized across jurisdictions to the greatest extent possible.

The FATF reviews money laundering and terrorist financing techniques and countermeasures; provides a forum for exchange of best practices; highlights areas of common concern; and promotes and monitors the progress of its members in adopting and implementing regulatory measures globally. In collaboration with other international stakeholders, the FATF also works to identify national-level vulnerabilities as part of its peer review process with the aim of protecting the international financial system from misuse, as well as creating standards for national best practices.

The FATF Recommendations and Virtual Asset Guidance. The FATF has developed a series of “Recommendations” that are recognized as the international standards for combating money laundering, terrorist financing, and the proliferation of weapons of mass destruction. FATF member countries are responsible for implementing the standards at the national level for compliance by the private sector. This provides the foundation for a coordinated international response aimed at confronting these threats to the integrity of the global financial system.

In 2014, the FATF recognized the need to bring virtual-asset-related activities within its scope, and in 2015 issued global guidance as part of a staged approach to addressing the money-laundering and terrorist-financing risks associated with virtual asset payment products and services. In July 2018, the FATF published a report at the G20 Finance Ministers and Central Bank Governors’ meeting outlining the FATF’s

commitment to addressing illicit finance threats involving virtual assets. Under the leadership of the United States, which held the FATF presidency at the time, the FATF in October 2018 updated its standards to clarify their application to virtual asset activities by amending “Recommendation 15” and adding two new glossary definitions—“virtual asset” and “virtual asset service provider.” Recommendation 15, which covers new technologies, states:

To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.¹⁴⁹

On June 21, 2019, the FATF adopted and issued a revised Interpretive Note to Recommendation 15 (“INR. 15”) that further clarifies and expands upon the FATF’s amendments to the standards relating to virtual assets, and describes how countries and obliged entities must comply with the relevant Recommendations to prevent the misuse of virtual assets for money laundering, terrorist financing, and proliferation.¹⁵⁰ Along with updated and expanded guidance aimed at assisting international jurisdictions and the private sector in implementing a risk-based approach to virtual assets and VASPs, INR. 15 requires countries to ensure that VASPs assess and mitigate their money laundering and terrorist financing risks, and implement

the full range of AML/CFT preventive measures under the Recommendations—just like other entities subject to AML/CFT regulation. These measures include customer due diligence, record keeping, suspicious transaction reporting, and screening of transactions for compliance with targeted financial sanctions, among others.¹⁵¹

Interaction with the Department of Justice.

The United States is a founding member of the FATF and, while holding the FATF presidency from July 2018 through June 2019, made it a priority to regulate VASPs for AML/CFT. The U.S. delegation to the FATF is led by the Department of the Treasury’s Office of Terrorist Financing and Financial Crimes, and includes the Department of Justice as a key interagency partner. The delegation urged that all FATF Recommendations broadly apply to VASPs and virtual asset financial activities, which resulted in the successful adoption of the amendments to Recommendation 15 along with the Interpretive Note and guidance discussed above. Department of Justice attorneys provided significant contributions to the drafting and adoption process for these important changes to the FATF standards. The FATF also pursues ongoing work on trends in AML/CFT risk related to virtual assets, such as publicly identifying red flags in virtual asset financial activity, and issuing reports that provide case studies drawn from all over the FATF’s global network. The Department of Justice has been an integral partner in this effort, providing analysis and case examples for the U.S. delegation.

III. Ongoing Challenges and Future Strategies

Parts I and II of this Framework discussed some of the serious public safety challenges posed by the misuse of cryptocurrency, and the legal and regulatory authorities the Department of Justice and its partners have used to address those challenges. This final Part explores the obligations of certain business and other entities that are particularly susceptible to abuse in the cryptocurrency space, and describes the Department's ongoing strategies for addressing these emerging threats to the safe and effective operation of the cryptocurrency marketplace.

A. Business Models and Activities That May Facilitate Criminal Activity

As described above, certain MSBs and other types of VASPs play a key role in the cryptocurrency ecosystem. Given their potential to facilitate criminal activity, these entities have a heightened responsibility to safeguard their platforms and businesses from exploitation by nefarious actors and to ensure that customer data is protected and secured. Moreover, the proper collection and maintenance of customer and transactional information by MSBs and other financial institutions pursuant to the BSA is crucial to the Department's ability to identify illicit actors, investigate criminal activity, and obtain evidence necessary for prosecutions. Key industry participants bearing these responsibilities include not only conventional virtual asset exchanges and brokers, but also peer-to-peer exchangers, kiosk operators,

and online casinos, as discussed further below. Unfortunately, many entities in these new and growing sectors often fail to comply, in whole or in part, with the BSA and other legal requirements, thereby threatening the Department's investigative abilities and undermining public safety.

Cryptocurrency exchanges. Companies and individuals that offer cryptocurrency and other virtual asset exchange services to the public are commonly referred to as "exchanges" and "exchangers." Even exchanges that do not accept fiat currency and operate only with cryptocurrency are obliged to follow FinCEN record keeping and reporting requirements, as the applicable regulations cover transfers of value and are not specific to fiat transactions. Moreover, all entities, including foreign-located exchanges, that do business wholly or in substantial part within the United States, such as by servicing U.S. customers, must also register with FinCEN and have an agent physically present in the United States for BSA reporting and for accepting service of process.¹⁵²

Peer-to-peer exchangers and platforms. Individuals seeking to buy or sell cryptocurrency other than through registered or licensed exchanges and financial institutions frequently turn to networks of individuals commonly referred to as peer-to-peer ("P2P") exchangers or traders. As individuals who facilitate transfers of value for the public, including the buying and selling of cryptocurrency, P2P exchangers are considered MSBs and are subject to FinCEN record keeping and reporting requirements.¹⁵³ In practice, however, many

Cryptocurrency Exchanges

- Allow users to buy and sell cryptocurrencies
- Serve as a conduit to the traditional financial system
- Can convert cryptocurrency to other virtual currencies or to fiat currency
- Global entities that can move money in seconds, not days
- In the U.S., exchanges are regulated by FinCEN as money service businesses
- In the international space, exchanges are subject to inconsistent regulatory regimes

P2P exchangers fail to register with FinCEN as MSBs or to comply with BSA obligations, and some even conduct transactions without requiring any form of identification from the customer.

P2P exchangers usually charge substantially higher percentage rates or fees—or use less favorable exchange rates—than registered exchanges. They often will accept a wide variety of payment methods, including payments of fiat currency in person or through the mail, deposits into bank accounts, Western Union or MoneyGram transfers, or payments in gift cards or stored value cards. P2P exchangers generally find their customers through word of mouth, open source websites such as Craigslist, or online exchange platforms.

P2P exchangers commonly use online exchange platforms or websites that allow users to trade virtual assets directly with one another and without a central operator. Nonetheless, when engaging in the transmission of virtual assets, these platforms must comply with BSA requirements. Although many P2P exchange platforms offer services similar to those offered by centralized

virtual asset exchanges, P2P exchange platforms provide opportunities for cross-platform trading of cryptocurrency without the use of traditional financial institutions. Furthermore, unlike centralized virtual asset exchanges, P2P exchange platforms may operate without an intermediary that will accept and transmit virtual assets in exchange for fiat or another type of virtual asset, or that will collect customer identification information. Individual exchangers—as well as platforms and websites—that fail to collect and maintain customer or transactional data or maintain an effective AML/CFT program may be subject to civil and criminal penalties.¹⁵⁴

Cryptocurrency kiosks. Cryptocurrency kiosks, which are commonly referred to as “Bitcoin ATMs,” are stand-alone machines that allow users to convert fiat currency to and from bitcoin and other cryptocurrencies. With these machines, cryptocurrency can be bought or sold directly using a customer’s mobile device or delivered in the form of a paper wallet. Thus, cryptocurrency kiosks offer an easy-to-use physical access point for virtual asset exchange.

Cryptocurrency Kiosks (aka Bitcoin ATMs)

- ATM-like machines that facilitate the buying, selling, and/or exchange of bitcoin or other cryptocurrencies
- Can be located almost anywhere, including malls, convenience stores, gas stations, and grocery stores
- Often charge much higher transaction fees for services than other types of cryptocurrency exchanges
- Capture different types of identifying information, including photographs or video
- Kiosk operators are considered money service businesses and are subject to anti-money laundering regulations and other legal requirements



Cryptocurrency kiosk operators are considered MSBs in the United States. Accordingly, they are subject to the BSA and must register with FinCEN and follow all applicable money transmission requirements, including collecting and maintaining KYC data on their clients,¹⁵⁵ reporting suspicious transactions to FinCEN, filing currency transaction reports for fiat transactions of \$10,000 or more in cash, and maintaining an effective AML/CFT program. While some operators comply with these requirements, many kiosks are not BSA-compliant and fail to collect required customer and transaction

information. Indeed, investigators have linked such kiosks to illicit use by drug dealers, credit card fraud schemers, prostitution rings, and unlicensed virtual asset exchangers.

Virtual currency casinos. The rising popularity of virtual assets has led to the growth of virtual-currency-based “casinos” that facilitate various forms of betting denominated in bitcoin and other virtual currencies. Under current law, a casino that has gross annual gaming revenue in excess of \$1 million must be duly licensed

HEROCOIN

On July 22, 2020, the Department of Justice announced that a California man agreed to plead guilty to operating an illegal virtual-currency money services business called Herocoin that exchanged up to \$25 million—including proceeds of criminal activity—through in-person transactions and a network of Bitcoin ATM-type kiosks. The kiosks were installed in malls, gas stations, and convenience stores throughout California, and allowed customers to exchange cash for bitcoin and vice versa. In his plea agreement, the defendant admitted that he intentionally failed to register Herocoin with FinCEN, and failed to implement an effective anti-money laundering program; file currency transaction reports for exchanges in excess of \$10,000; conduct due diligence on customers; or file suspicious activity reports. With respect to the Bitcoin ATM network, the defendant also admitted that he failed to implement a program to obtain identifications for customers conducting multiple transactions of up to \$3,000 or verify that any identification provided actually reflected the person conducting the transaction. After pleading guilty, the defendant will face a statutory maximum sentence of 30 years in federal prison, and will forfeit cash, cryptocurrency, and 17 Bitcoin ATMs.¹⁵⁶

Figure 13: Image of Cryptocurrency Kiosks Seized in the Herocoin Case



or authorized to do business as a casino in the United States by a federal, State, or tribal authority.¹⁵⁷ Casinos that do not meet this criterion are considered MSBs. Whether regulated as casinos or MSBs, these gambling businesses are subject to the BSA and its KYC record keeping and reporting requirements. Traditional brick-and-mortar casinos generally do not accept bitcoin or other cryptocurrencies; however, online gambling sites increasingly do accept cryptocurrencies. Online casinos that provide gambling services are also MSBs and must comply with applicable money transmission regulations. Although many do not have a known physical location, they still are required to report suspicious transactions to FinCEN if they offer services to U.S. customers.

Anonymity enhanced cryptocurrencies.

The acceptance of anonymity enhanced cryptocurrencies or “AECs”—such as Monero, Dash, and Zcash—by MSBs and darknet marketplaces has increased the use of this type of virtual currency. As discussed above, because AECs use non-public or private blockchains, use of these cryptocurrencies may undermine the AML/CFT controls used to detect suspicious activity by MSBs and other financial institutions, and may limit or even negate a business’s ability to conduct AML/CFT checks on customer activity and to satisfy BSA requirements. Some AECs, however, offer features, such as public view keys, that potentially can facilitate the fulfillment of AML/CFT obligations, depending upon the implementation of such features.

The Department considers the use of AECs to be a high-risk activity that is indicative

of possible criminal conduct. In most circumstances, the Department does not liquidate seized or forfeited AECs, as doing so allows them to re-enter the stream of commerce for potential future criminal use. Companies that choose to offer AEC products should consider the increased risks of money laundering and financing of criminal activity, and should evaluate whether it is possible to adopt appropriate AML/CFT measures to address such risks.

AECs are often exchanged for other virtual assets like bitcoin, which may indicate a cross-virtual-asset layering technique for users attempting to conceal criminal behavior. This practice, which is commonly referred to as “chain hopping,” is discussed further below.

Mixers, tumblers, and chain hopping.

“Mixers” and “tumblers” are entities that attempt to obfuscate the source or owner of particular units of cryptocurrency by mixing the cryptocurrency of several users prior to delivery of the units to their ultimate destination. For a fee, a customer can send cryptocurrency to a specific address that is controlled by the mixer. The mixer then commingles this cryptocurrency with funds received from other customers before sending it to the requested recipient address. Websites or companies offering mixing or tumbling services are engaged in money transmission, and therefore are MSBs subject to the BSA and other similar international regulations. In addition to facing BSA liability for failing to register, conduct AML procedures, or collect customer identification, operators of these services can be criminally liable for money laundering because these mixers and tumblers are designed specifically to

Figure 14: Example of a Criminal “Mixing” Enterprise

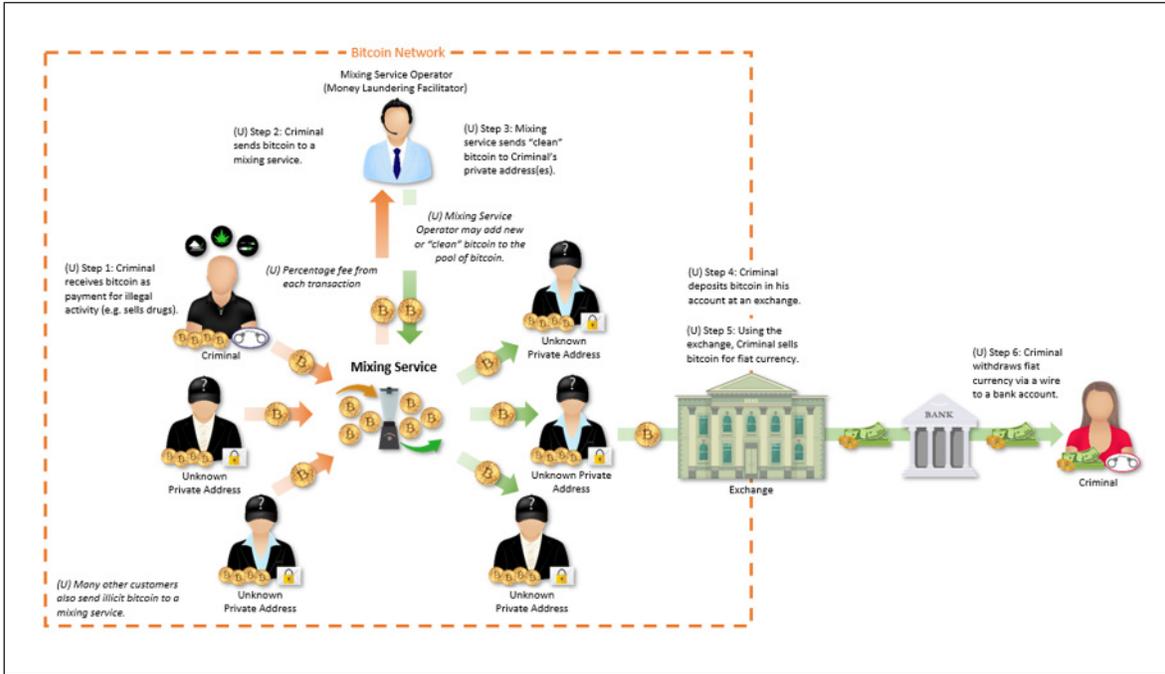
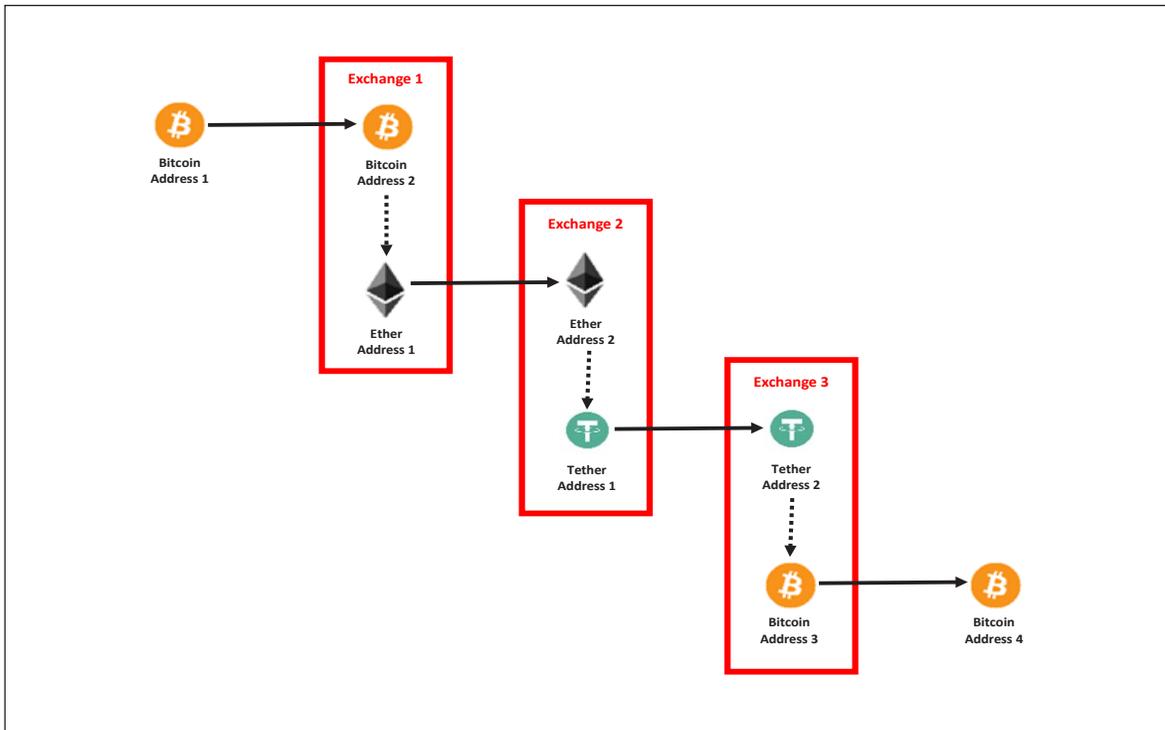


Figure 15: Illustration of “Chain Hopping”

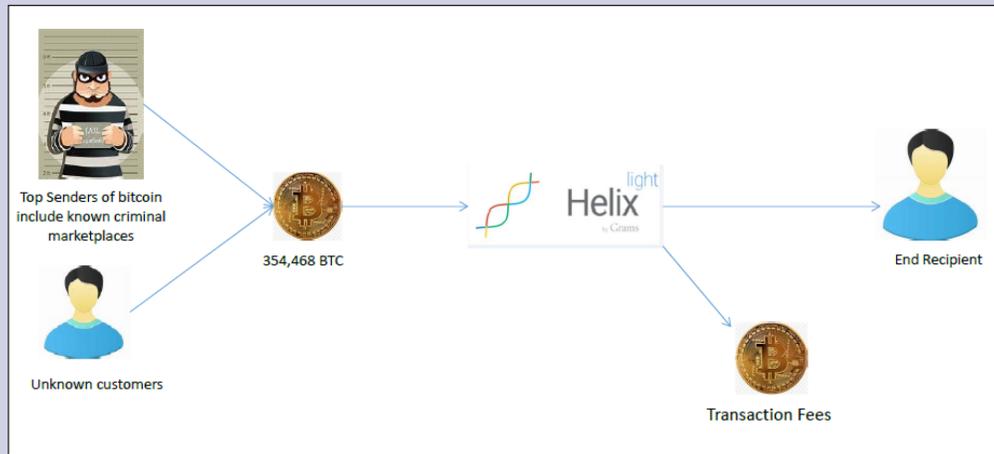


HELIX

On February 13, 2020, the Department of Justice announced the indictment and arrest of the alleged administrator of Helix, a darknet cryptocurrency laundering service. According to the indictment, Helix functioned as a bitcoin “mixer” or “tumbler,” allowing customers to send bitcoin to designated recipients in a manner that was designed to conceal their source or owner.

The service’s administrator is alleged to have advertised Helix to customers on the darknet as a way to conceal transactions from law enforcement. The indictment charges Helix with laundering over \$300 million of bitcoin, which allegedly represented the proceeds of illicit narcotics sales and other criminal transactions.¹⁵⁸

Figure 16: Helix Allegedly “Tumbled” a Large Volume of Bitcoin, Charging a Fee for Each Transaction



Helix allegedly received more than 354,468 bitcoin between the site’s launch in June 2014 and December 2017, valued at approximately \$311 million in U.S. dollars at the time of the transactions.

“conceal or disguise the nature, the location, the source, the ownership, or the control” of a financial transaction.¹⁵⁹

Criminals also may engage in a practice known as “chain hopping,” in which they move from one cryptocurrency to another, often in rapid succession. As the Department has observed, chain hopping is “frequently used by individuals who are laundering proceeds of virtual currency thefts.”¹⁶⁰ Chain hopping is often viewed as a potential way to obfuscate the trail of virtual currency by shifting the trail of transactions from the blockchain of one virtual currency to the blockchain of another virtual currency.

Jurisdictional arbitrage and compliance deficiencies. Because of the global and cross-border nature of transactions involving virtual assets, the lack of consistent AML/CFT regulation and supervision over VASPs across jurisdictions—and the complete absence of such regulation and supervision in certain parts of the world—is detrimental to the safety and stability of the international financial system.¹⁶¹ This inconsistency also impedes law enforcement’s ability to investigate, prosecute, and prevent criminal activity involving or facilitated by virtual assets. For example, illicit financial flows denominated in virtual assets may move to companies and exchanges in jurisdictions where authorities lack regulatory frameworks requiring the generation and retention of records necessary to support investigations.

In the United States, AML/CFT standards have been in place for MSBs engaged in virtual asset activities since 2011, and yet many VASPs still are operating in ways

that do not comply with the BSA and other regulatory requirements. For example, some VASPs apply different standards to U.S. customers versus customers in other countries, while other VASPs actively apply different standards to virtual-asset-to-fiat transactions than to virtual-asset-to-virtual-asset transactions. Such behaviors are flatly inconsistent with VASPs’ BSA obligations and can create significant financial intelligence gaps.

B. Department of Justice Response Strategies

Investigations and prosecutions generally. Consistent with its mission to protect public safety and national security, the Department of Justice will continue its aggressive investigation and prosecution of a wide range of malicious actors, including those who use cryptocurrencies to commit, facilitate, or conceal their crimes. For instance, the Department has prosecuted a number of individuals operating as P2P exchangers for money laundering and for violating the BSA.¹⁶² Many of these exchangers were selling virtual assets that they obtained from their own involvement in other criminal activities, such as drug trafficking or computer hacking, or were otherwise knowingly facilitating the criminal activities of others.

As discussed above, the Department has a broad range of legal authorities for investigating and prosecuting individuals who misuse cryptocurrency for criminal purposes. To that end, the Department is committed to an appropriate all-tools approach to dealing with cryptocurrency-related crime. The Department will continue

to engage actively with its regulatory partners to address the misuse and abuse of cryptocurrency by malicious actors. The case examples noted throughout this Framework highlight the many successes from the Department's work with regulatory partners such as FinCEN, OFAC, the SEC, the CFTC, and the IRS. By appropriately coordinating parallel enforcement actions, the Department can maximize its impact in investigating, dismantling, and deterring criminal activity; more effectively recover funds for victims; and better safeguard the financial system and the American public.

The Department also has robust authority to prosecute VASPs and other entities and individuals that violate U.S. law even when they are not located inside the United States. Where virtual asset transactions touch financial, data storage, or other computer systems within the United States, the Department generally has jurisdiction to prosecute the actors who direct or conduct those transactions. The Department also has jurisdiction to prosecute foreign-located actors who use virtual assets to import illegal products or contraband into the United States, or use U.S.-located VASPs or financial institutions for money laundering purposes. In addition, the Department may prosecute for violations of U.S. law those foreign-located actors who provide illicit services to defraud or steal from U.S. residents. Moreover, as FinCEN has observed, the BSA applies to entities and individuals that engage in money transmission as a business and that operate wholly or substantially in part in the United States, regardless of where they are incorporated or headquartered.

Finally, it bears emphasizing that if conduct involving virtual currency were to violate the U.S. statutes regarding material support of terrorism, the U.S. government could appropriately assert jurisdiction over such offenses anywhere in the world, consistent with due process, under the principle of protective jurisdiction. That principle holds that “[f]or non-citizens acting entirely abroad, a jurisdictional nexus exists when the aim of that activity is to cause harm inside the United States or to U.S. citizens or interests.”¹⁶³ Where a malign actor's conduct involving cryptocurrency amounts to providing material support to a designated foreign terrorist organization, that actor engages in conduct that threatens the security of the United States, and therefore subjects himself (or itself) to the jurisdiction of our Nation's courts—and to the Department's enforcement of the Nation's laws.¹⁶⁴

Promoting law enforcement awareness and expertise. Given the complexity of cryptocurrency technology and of the platforms on which it is used, law enforcement professionals across agencies must continually develop and maintain the base of knowledge and skills necessary to identify threats involving cryptocurrency; conduct robust and efficient investigations of those threats; and employ the many appropriate legal tools available to bring individuals and entities that abuse cryptocurrency to justice. The Department is taking the lead in this area by dedicating resources to existing initiatives and groups that encourage law enforcement awareness and expertise in the cryptocurrency space. These efforts include continuing to promote Department-wide,

CASE STUDY: BTC-e

The BTC-e case, which was introduced earlier,¹⁶⁵ is one example of the Department of Justice's resolve to prosecute foreign-located entities and individuals in the cryptocurrency context. BTC-e operated globally as an unlicensed virtual currency exchange to launder and liquidate criminal proceeds from virtual currency to fiat currency. In doing so, it relied on the use of shell companies and affiliated entities that were similarly unregistered with FinCEN. According to its now-defunct website, BTC-e purported to be based in Eastern Europe. BTC-e's managing shell company, Canton Business Corporation, was registered in the Seychelles, and its web domains were registered to shell companies in, among other places, Singapore, the British Virgin Islands, France, and New Zealand. After a multi-year, multi-agency investigation, the Department successfully charged BTC-e and one of its principal operators with operating an unlicensed money services business, money laundering, and other related crimes.



Figure 17: BTC-e Website after Seizure by the U.S. Government

CASE STUDY: ALPHABAY

The AlphaBay case, which also was mentioned previously,¹⁶⁶ further demonstrates the global reach of the Department of Justice, U.S. law enforcement, and our domestic and international partners in identifying and neutralizing unlawful activities involving cryptocurrency. At the time of its takedown by law enforcement in July 2017, AlphaBay was the dark web's largest criminal marketplace, serving over 200,000 users as a conduit for everything from illegal drugs and firearms to malware and toxic chemicals. Aided by the use of cryptocurrencies like Bitcoin, Monero, and Ether, AlphaBay's operators were able to hide the location and identities of the site's administrators and users and to facilitate the laundering of hundreds of millions of dollars. Over the course of the government's investigation, law enforcement identified AlphaBay proceeds and discovered hundreds of thousands of cryptocurrency addresses associated with the site.¹⁶⁷ The international operation to dismantle AlphaBay was led by the United States and involved cooperation from law enforcement partners in Thailand, the Netherlands, Lithuania, Canada, the United Kingdom, and France, as well as the European law enforcement agency Europol.¹⁶⁸ The legal proceedings in the United States demonstrated the breadth of authorities the Department can and will bring to bear in appropriate cases.¹⁶⁹



THE DIGITAL CURRENCY INITIATIVE

As announced in the July 2018 Report of the Attorney General’s Cyber Digital Task Force, the Money Laundering and Asset Recovery Section (“MLARS”) within the Department of Justice’s Criminal Division has established a Digital Currency Initiative to focus on “providing support and guidance to investigators, prosecutors, and other government agencies on cryptocurrency prosecutions and forfeitures.”¹⁷¹ The Digital Currency Initiative continues to “expand and implement cryptocurrency-related training to encourage and enable more investigators, prosecutors, and Department components to pursue such cases, while developing and disseminating policy guidance on various aspects of cryptocurrency, including seizure and forfeiture.”¹⁷²

consider legislative proposals to close any existing gaps in enforcement authority.

Fostering cooperation with State authorities. As discussed above, State attorneys general offices and regulatory agencies play an important role in protecting the investing public by enforcing State securities laws and licensing, registration, and auditing requirements. Coordination and de-confliction with State attorneys general offices, regulators, and prosecuting entities is crucial, and yet communication on matters involving virtual assets between federal prosecutors and State authorities currently varies by jurisdiction. United States Attorneys’ Offices and Department litigating divisions should continue to develop lines of communication with State authorities handling securities and fraud investigations, prosecutions, and enforcement actions involving cryptocurrency and virtual-asset-related investment products. In addition, Department agencies should communicate and coordinate with State financial and banking authorities that regulate money transmitters operating in their respective

jurisdictions to prevent conflicts and duplication of efforts in money laundering prosecutions.

Enhancing international cooperation and promoting comprehensive and consistent international regulation. The inherently global nature of the virtual asset ecosystem poses significant investigative challenges for U.S. law enforcement agencies and for Department prosecutors. Effectively countering criminal activity involving virtual assets requires close international partnerships. Foreign partners assist U.S. law enforcement in, for example, conducting investigations, making arrests, and seizing criminal assets. Similarly, foreign partners may rely on the assistance of U.S. law enforcement to take action against individuals who commit crimes abroad and conceal evidence and assets—or themselves—within the United States. The Department will continue to encourage these partnerships in support of multi-jurisdictional parallel investigations and prosecutions, particularly those involving foreign-located actors, VASPs, and transnational criminal organizations.

THE GDPR

In May 2018, the European Union (“EU”) General Data Protection Regulation 2016/679 (“GDPR”) came into effect. GDPR is a sweeping data protection and privacy law that applies to all data controllers, data processors, and data subjects within the EU’s jurisdiction. Some virtual currency exchanges have attempted to withhold data requested by law enforcement agencies in the United States through criminal grand jury subpoenas by citing GDPR’s broad privacy rules.

However, GDPR does not in fact bar companies subject to U.S. jurisdiction from complying with lawful requests in criminal investigations. To the contrary, GDPR explicitly permits the disclosure of data in a number of scenarios. For example, a virtual exchange that is subject to GDPR may process the requested data under GDPR Article 6(1) when “necessary for compliance with a legal obligation to which the controller is subject” or “necessary for the purposes of the legitimate interests pursued by the controller or by a third party”¹⁷³ Similarly, under Article 49.1, international transfer of data is permitted in various circumstances, including where “the transfer is necessary for important reasons of public interest” or “necessary for the purposes of compelling legitimate interests pursued by the controller.”¹⁷⁴

The ability of law enforcement to investigate criminal activity is plainly an important reason of public interest, placing production of records pursuant to U.S. grand jury subpoenas squarely within the “public interest” exception in Article 49.1. Moreover, the transfer of data from exchanges may constitute a “compelling legitimate interest” in that the transfer may be necessary to prevent or defend against being held in contempt of court for failure to respond to lawful process. Indeed, the European Commission itself recognized this framework in a 2017 amicus brief it filed in the U.S. Supreme Court in *United States v. Microsoft*,¹⁷⁵ which discussed the GDPR’s rules governing the transfer of personal data to a non-EU state. In its brief, the European Commission recognized that the public interest is served by transferring data to non-EU countries to further international criminal investigations, stating: “[I]n general, [European] Union as well as Member State law recognize the importance of the fight against serious crime—and thus criminal law enforcement and international cooperation in that respect—as an objective of general interest.”¹⁷⁶

GDPR Articles 6 and 49.1 provide additional legal bases for processing and transfer that may be applicable in particular circumstances. For example, Article 49.1(e) establishes a derogation if “the transfer is necessary for the establishment, exercise or [defense] of legal claims.”¹⁷⁷ This derogation may be applicable where the transfer of data from exchanges is sought pursuant to a subpoena or other compulsory order.

While the Department disagrees with the basis for such objections to lawful requests for information, some exchanges continue to cite to the GDPR while refusing to comply with standard grand jury subpoenas. The Department will continue to engage with these virtual currency exchanges to ensure compliance with lawful requests and will pursue motions to compel as needed.

The Department also works with its partners in the federal government to encourage their international counterparts to continue development of comprehensive and consistent international regulation of virtual assets. As discussed above, the Financial Action Task Force has adopted amendments to its Recommendation 15 that bring VASPs and virtual asset activity within the FATF's standards for AML/CFT. As implementation of these amendments expands across global jurisdictions, the Department will continue to provide policy support and subject matter expertise to the Department of the Treasury-led U.S. delegation, and to work internationally to level the legal and regulatory playing field related to virtual assets. In addition, other international organizations, including the United Nations Office on Drugs and Crime, are in the process of adopting regulatory frameworks that mirror the FATF's developing approach to virtual asset activity. We will monitor and actively contribute to those efforts, as appropriate.

Finally, the Department will continue to encourage its partners to support the adoption of consistent regulations across jurisdictions to prevent illicit actors from practicing jurisdictional arbitrage, and to ensure the collection of important evidence and seizure of illicit assets regardless of where an entity or illicit actor may be operating.

Conducting private sector education and outreach. As with any specialized, technology-driven industry, effective regulation and policing of cryptocurrency activity requires close cooperation between the public and private sectors whenever

possible. This approach includes direct engagement with the companies that operate in the virtual asset space; with the banks and financial institutions that may be affected by virtual asset regulation; and, importantly, with the actual community of cryptocurrency users. In conducting such outreach, the Department and its partners will continue their efforts to advance mutual goals such as safeguarding the virtual asset marketplace from theft, fraud, and hacking.

Conclusion

As the use of cryptocurrency evolves and expands, so too will opportunities to commit crime and to do harm by exploiting cryptocurrency technology. Every day, criminals expand and perfect techniques designed to evade detection and apprehension. Ultimately, illicit uses of cryptocurrency threaten not just public safety, but national security, as well. For example, cryptocurrency can provide terrorist organizations a tool to circumvent traditional financial institutions in order to obtain, transfer, and use funds to advance their missions. Current terrorist use of cryptocurrency may represent the first raindrops of an oncoming storm of expanded use that could challenge the ability of the United States and its allies to disrupt financial resources that would enable terrorist organizations to more successfully execute their deadly missions or to expand their influence.

Likewise, cryptocurrency presents a troubling new opportunity for individuals and rogue states to avoid international sanctions and to undermine traditional financial markets,

thereby harming the interests of the United States and its allies.

Despite the many challenges, the Department of Justice has aggressively investigated and prosecuted a range of malign actors who have used cryptocurrencies to facilitate or to conceal their illicit activities. Similarly, the Department has brought actions against individuals and companies that have failed to meet their legal obligations to counter illicit activity. In particular cases, we have even proceeded against the illicit cryptocurrency itself, seizing those virtual assets and removing them from the stream of international commerce, irrespective of our ability to identify or to apprehend the actors who used them. This essential work will continue, as the Department seeks to ensure that uses of cryptocurrency adhere to the law and are compatible with the protection of public safety and national security.

The Department of Justice, however, cannot achieve success on its own. We recognize the importance of working with interagency and

international partners to enhance an already vigorous enforcement plan, regulatory scheme, and policy framework to thwart the opportunities created by cryptocurrency for criminals, terrorists, and other bad actors. The Department is committed to strengthening its key partnerships by promoting law enforcement awareness and expertise; by fostering cooperation with State authorities; by enhancing international cooperation; by promoting comprehensive, consistent international regulation; and by conducting private sector education and outreach.

To promote public safety and protect national security, all stakeholders—from private industry to regulators, elected officials, and individual cryptocurrency users—will need to take steps to ensure cryptocurrency is not used as a platform for illegality. Indeed, for cryptocurrency to realize its truly transformative potential, it is imperative that these risks be addressed.



NOTES

Introduction

ⁱ The original formulation of this phrase (describing the laws as “those wise restraints that make men free”) was coined by Professor John MacArthur Maguire of Harvard. See <https://asklib.law.harvard.edu/faq/115309> (last accessed Oct. 1, 2020).

ⁱⁱ Jeff Sessions, Attorney General, “Memorandum for Heads of Department Components [Establishing Cyber-Digital Task Force],” Feb. 16, 2018, available at: <https://www.justice.gov/opa/press-release/file/1035457/download> (last accessed Oct. 1, 2020).

ⁱⁱⁱ U.S. DEP’T OF JUSTICE, REPORT OF THE ATTORNEY GENERAL’S CYBER-DIGITAL TASK FORCE 126 (2018), available at: <https://www.justice.gov/cyberreport> (last accessed Oct. 1, 2020).

^{iv} U.S. DEP’T OF COMMERCE, NAT’L INST. OF STANDARDS AND TECH., “Blockchain,” available at: <https://www.nist.gov/topics/blockchain> (last accessed Oct. 1, 2020).

^v U.S. DEP’T OF DEF, “DoD Digital Modernization Strategy,” at 44 (Appendix I), July 12, 2019, available at: <https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF> (last accessed Oct. 1, 2020).

^{vi} See U.S. FOOD AND DRUG ADMIN., “New Era of Smarter Food Safety: FDA’s Blueprint for the Future,” July 2020, available at: <https://www.fda.gov/media/139868/download> (last accessed Oct. 1, 2020).

^{vii} Lael Brainard, Fed. Reserve Governor, “An Update on Digital Currencies,” Aug. 13, 2020, available at: <https://www.federalreserve.gov/newsevents/speech/brainard20200813a.htm> (last accessed Oct. 1, 2020).

^{viii} BINANCE, “The Evolution of the Internet – Web 3.0 Explained,” Feb. 2020, available at: <https://academy.binance.com/en/articles/the-evolution-of-the-internet-web-3-0-explained> (last accessed Oct. 1, 2020).

Cryptocurrency: An Enforcement Framework

¹ CTRS. FOR DISEASE CONTROL & PREVENTION, *Drug Overdose Deaths*, <https://www.cdc.gov/drugoverdose/data/statedeaths.html> (last accessed Oct. 1, 2020).

² FINANCIAL ACTION TASK FORCE (FATF), THE FATF RECOMMENDATIONS: INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION 126 (June 2019) [hereinafter FATF INTERNATIONAL STANDARDS], available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> (last accessed Oct. 1, 2020).

³ Some countries, including the United States (see text accompanying *supra* note vii), are exploring the use of blockchain technology to support a national currency. Such currencies are sometimes referred to as “Central Bank Digital Currencies” or “CBDCs.” See, e.g., PRICEWATERHOUSECOOPERS, THE RISE OF CENTRAL BANK DIGITAL CURRENCIES (CBDCs) 2 (Nov. 2019), available at: <https://www.pwc.com/gx/en/financial-services/pdf/the-rise-of-central-bank-digital-currencies.pdf> (last accessed Oct. 1, 2020).

⁴ U.S. DEPT. OF THE TREASURY, FIN. CRIMES ENF'T NETWORK, FINCEN GUIDANCE FIN-2013-G001, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES (Mar. 18, 2013), available at: <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf> (last accessed Oct. 1, 2020). A non-convertible virtual currency may effectively become a convertible virtual currency where a robust unofficial secondary market for the currency develops and provides the opportunity to exchange the "non-convertible" currency for fiat or other virtual currency. See FINANCIAL ACTION TASK FORCE (FATF), VIRTUAL CURRENCIES: KEY DEFINITIONS AND POTENTIAL AML/CFT RISKS 4–5 (June 2014), available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> (last accessed Oct. 1, 2020).

⁵ Throughout this publication, specific examples of cryptocurrency, like Bitcoin, are capitalized when referring to the protocol, and lowercase when referring to units of the cryptocurrency.

⁶ To the extent this Framework discusses or references criminal cases that are pending at the time of publication, it should be noted that criminal charges are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

⁷ For example, Christopher Bantli, a Canadian citizen, used cryptocurrency while acting as a vendor of controlled substances on the darknet website AlphaBay. In February 2019, Bantli pleaded guilty in U.S. federal court to accepting virtual currency as payment for controlled substances, including powerful fentanyl analogues and synthetic opiates. See Press Release, "Dark Web Trafficker Convicted of Drug Importation Conspiracy," U.S. DEPT. OF JUSTICE

(Feb. 13, 2019), available at: <https://www.justice.gov/opa/pr/dark-web-trafficker-convicted-drug-importation-conspiracy> (last accessed Oct. 1, 2020).

⁸ In October 2018, Ammar Atef Alahdali pleaded guilty to receipt of child pornography after admitting to paying cryptocurrency to become a member of a darknet website dedicated to the advertisement and distribution of such illicit material. In 2017, Alahdali used the website to download more than twenty images depicting the sexual abuse of children, including at least one video depicting sadistic sexual conduct. See Press Release, "Foreign National Pleads Guilty to Downloading Child Pornography from the Dark Web in Exchange for Cryptocurrency," U.S. DEPT. OF JUSTICE (Oct. 2, 2018), available at: <https://www.justice.gov/opa/pr/foreign-national-pleads-guilty-downloading-child-pornography-dark-web-exchange-cryptocurrency> (last accessed Oct. 1, 2020).

⁹ For examples of cases where cryptocurrencies were used in the illicit sales on the dark web, see, e.g., *United States v. Hagan*, 766 Fed. Appx. 356 (6th Cir. 2019) (MDMA, LSD, DMT, mushrooms, and marijuana); *United States v. Reuer*, CR. 19-50022-JLV, 2019 WL 1012187 (D.S.D. Mar. 4, 2019) (methamphetamine, fentanyl, and heroin); *State v. Sawyer*, 187 A.3d 377 (Vt. 2018) (firearms); *State v. A.P.*, 117 N.E.3d 840 (Ohio 2018) (LSD); *United States v. 2013 Lamborghini Aventador*, No. 1:17-cv-00967-ljo-sko, 2018 WL 3752131 (E.D. Cal. Aug. 8, 2018) (luxury vehicles); *United States v. Mitchell*, No. CR-17-01690-001-PHX-GMS, 2018 WL 2688803 (D. Ariz. June 5, 2018) (potassium cyanide and dimethyl mercury); *United States v. Vallerius*, No. 17-CR-20648, 2018 WL 2325729 (S.D. Fla. May 1, 2018) (narcotics); *United States v. Focia*, 869 F.3d 1269 (11th Cir. 2017) (firearms); *United States v. Ulbricht*, 858 F.3d 71 (2d Cir. 2017) (drugs, false identification documents, and computer hacking software);

United States v. Colldock, No. CR-16-1254-JAS, 2017 WL 9615895 (D. Ariz. Sept. 11, 2017) (methamphetamine and cocaine); *United States v. Levin*, 186 F. Supp. 3d 26 (D. Mass. 2016) (child pornography); *United States v. Parks*, No. S1-4:15 CR 553, 2016 WL 6775465 (E.D. Mo. Sept. 19, 2016) (human trafficking and prostitution); *United States v. 50.44 Bitcoins*, No. ELH-15-3692, 2016 WL 3049166 (D. Md. May 31, 2016) (narcotics and illicit Bitcoin-to-fiat-currency exchanges); and *United States v. Donagal*, No. 14-cr-00285-JST-1, 2014 WL 6601843 (N.D. Cal. Nov. 18, 2014) (illegally manufactured Xanax, GHB, steroids, and other drugs).

¹⁰ See *infra* pages 7-20 (describing AlphaBay, Operation Disruptor, terrorist financing cases, and other examples).

¹¹ For example, in 2017, the U.S. government formally asserted that North Korea conducted a massive ransomware attack, referred to as the WannaCry attack, which infected computers around the world. The perpetrators of the WannaCry attack demanded ransom payments from their victims in Bitcoin. See, e.g., Thomas P. Bossert, *It's Official: North Korea Is Behind WannaCry*, WALL ST. J., Dec. 18, 2017, available at: <https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537> (last accessed Oct. 1, 2020).

¹² Press Release, “FBI Expects a Rise in Scams Involving Cryptocurrency Related to the COVID-19 Pandemic,” FEDERAL BUREAU OF INVESTIGATION (Apr. 13, 2020), available at: <https://www.fbi.gov/news/pressrel/press-releases/fbi-expects-a-rise-in-scams-involving-cryptocurrency-related-to-the-covid-19-pandemic#:~:text=FBI%20Expects%20a%20Rise%20in%20Scams%20Involving%20Cryptocurrency%20Related%20to,through%20the%20complex%20cryptocurrency%20ecosystem> (last accessed Oct. 1, 2020).

¹³ See *infra* page 16.

¹⁴ In what was reported in January 2015 as the “first instance of an ISIS cell fundraising using Bitcoin on the dark web,” the FBI shut down the online cryptocurrency account of a known ISIS fundraiser, Abu Mustafa. Zachary K. Goldman, Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, & Julia Solomon-Strauss, *Terrorist Use of Virtual Currencies: Containing the Potential Threat*, CTR. FOR A NEW AM. SEC., May 2017, at 12, available at: <https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-TerroristFinancing-Final.pdf?mtime=20170502033819> (last accessed Oct. 1, 2020); see also European Parliament Policy Department for Citizens’ Rights and Constitutional Affairs, *Virtual Currencies and Terrorist Financing: Assessing Risks and Evaluating Responses*, May 2018, available at: [https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU\(2018\)604970_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf) (providing detailed threat assessment, describing European Union’s response, and setting out policy recommendations) (last accessed Oct. 1, 2020).

¹⁵ Press Release, “Virginia Man Sentenced to More Than 11 Years for Providing Material Support to ISIL,” U.S. DEPT. OF JUSTICE (Aug. 28, 2015), available at: <https://www.justice.gov/opa/pr/virginia-man-sentenced-more-11-years-providing-material-support-isil> (last accessed Oct. 1, 2020).

¹⁶ Press Release, “Global Disruption of Three Terror Finance Cyber-Enabled Campaigns,” U.S. DEPT. OF JUSTICE (Aug. 13, 2020), available at: <https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns> (last accessed Oct. 1, 2020).

¹⁷ See Press Release, “Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals,

Municipalities, and Public Institutions, Causing Over \$30 Million in Losses,” U.S. DEPT. OF JUSTICE (Nov. 28, 2018), available at: <https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public> (last accessed Oct. 1, 2020). The charges in the indictment are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

¹⁸ Press Release, “South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin,” U.S. DEPT. OF JUSTICE (Oct. 16, 2019), available at: <https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child> (last accessed Oct. 1, 2020). The charges in the indictment are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

¹⁹ Indictment, *United States v. Mohammad*, No. 20-cr-0065, at 6 (DLF) (D.D.C. March 2020), available at: <https://www.justice.gov/usao-dc/press-release/file/1257641/download> (last accessed Oct. 1, 2020); *see also* Press Release, “Dutch National Charged in Takedown of Obscene Website Selling Over 2,000 ‘Real Rape’ and Child Pornography Videos, Funded by Cryptocurrency,” U.S. DEPT. OF JUSTICE (Mar. 12, 2020), available at: <https://www.justice.gov/usao-dc/pr/dutch-national-charged-takedown-obscene-website-selling-over-2000-real-rape-and-child> (last accessed Oct. 1, 2020). The charges in the indictment are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

²⁰ Verified Complaint for Forfeiture In Rem, *United States v. Three Hundred Three Virtual Currency Accounts et. al.*, No. 20-cv-712 (D.D.C. Mar. 12, 2020), available at: <https://www.justice.gov/usao-dc/press-release/file/1257581/download> (last accessed Oct. 1, 2020).

²¹ Press Release, “Global Disruption of Three Terror Finance Cyber-Enabled Campaigns,” *supra* note 16.

²² Verified Complaint for Forfeiture In Rem, *United States v. One Hundred Fifty Five Virtual Currency Assets*, No. 20-cv-2228 (D.D.C. Aug. 13, 2020), available at: <https://www.justice.gov/opa/press-release/file/1304296/download> (last accessed Oct. 1, 2020).

²³ Press Release, “‘Bitcoin Maven’ Sentenced to One Year in Federal Prison in Bitcoin Money Laundering Case,” U.S. DEPT. OF JUSTICE, U.S. ATT’Y’S OFFICE, C.D. CAL. (July 9, 2018), available at: <https://www.justice.gov/usao-cdca/pr/bitcoin-maven-sentenced-one-year-federal-prison-bitcoin-money-laundering-case> (last accessed Oct. 1, 2020).

²⁴ The federal crime of money laundering is defined in 18 U.S.C. § 1956.

²⁵ AML/CFT standards are discussed further in Part II.

²⁶ *See* FINCEN GUIDANCE FIN-2013-G001, *supra* note 4, at 2; *see also* VIRTUAL CURRENCIES: KEY DEFINITIONS AND POTENTIAL AML/CFT RISKS, *supra* note 4, at 7.

²⁷ Press Release, “‘Bitcoin Maven’ Sentenced to One Year,” *supra* note 23.

²⁸ Press Release, “Russian National And Bitcoin Exchange Charged In 21-Count Indictment For Operating Alleged International Money Laundering Scheme And Allegedly Laundering Funds From Hack Of Mt. Gox,” U.S. DEPT. OF JUSTICE, U.S. ATT’Y’S OFFICE, N.D. CAL. (July 26, 2017), available at: <https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged> (last accessed Oct. 1, 2020). The charges in the indictment are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

²⁹ For other examples of cases in which virtual currency exchanges have been charged with operating an unlicensed money transmitting business, see *United States v. Murgio*, 15-cr-769(AJN), 2017 WL 365496 (S.D.N.Y. Jan. 20, 2017) and *United States v. Faiella*, 39 F. Supp. 3d 544 (S.D.N.Y. 2014). See also *United States v. Budovsky*, No. 13-cr-368 (DLC), 2015 WL 5602853, at *14 (S.D.N.Y. Sept. 23, 2015) (noting that 18 U.S.C. § 1960, which covers operation of an unlicensed money transmitting business, encompasses businesses that transmit virtual currency).

³⁰ See I.R.S. Notice 2014-21, available at: <https://www.irs.gov/pub/irs-drop/n-14-21.pdf> (last accessed Oct. 1, 2020).

³¹ Press Release, “Treasury Sanctions Russia-based Bank Attempting to Circumvent U.S. Sanctions on Venezuela,” U.S. DEPT. OF THE TREASURY (Mar. 11, 2019), available at: <https://home.treasury.gov/news/press-releases/sm622> (last accessed Oct. 1, 2020).

³² See generally, e.g., Yaya J. Fanusie & Trevor Logan, *Crypto Rogues: U.S. State Adversaries Seeking Blockchain Sanctions Resistance*, FOUND. FOR DEF. OF DEMOCRACIES (July 2019),

available at: <https://www.fdd.org/wp-content/uploads/2019/07/fdd-report-crypto-rogues.pdf> (last accessed Oct. 1, 2020). While publicly available details remain scarce, reports indicate that North Korea also has been active in exploiting cryptocurrency technology in part because of “a desire to avoid crippling international sanctions.” Megan McBride & Zack Gold, *Cryptocurrency: Implications for Special Operations Forces* at 30, CNA (Aug. 2019), available at: https://www.cna.org/CNA_files/PDF/CRM-2019-U-020186-Final.pdf (last accessed Oct. 1, 2020); see also *Crypto Rogues*, *supra*, at 8 n.4 (“North Korea is also trying to obtain cryptocurrencies to offset sanctions mostly through cyber theft.”).

³³ Gertrude Chavez-Dreyfuss, *Cryptocurrency Crime Losses More than Double to \$4.5 Billion in 2019, Report Finds*, REUTERS, Feb. 11, 2020, available at: <https://www.reuters.com/article/us-crypto-currencies-crime/cryptocurrency-crime-losses-more-than-double-to-45-billion-in-2019-report-finds-idUSKBN2051VT> (last accessed Oct. 1, 2020).

³⁴ As discussed further in the text, the Department of Justice recently brought criminal charges against two individuals accused of laundering over \$100 million worth of cryptocurrency allegedly stolen by North Korean hacks of cryptocurrency exchanges. The Department also filed a civil forfeiture complaint that “publicly exposes the ongoing connections between North Korea’s cyber-hacking program and a Chinese cryptocurrency money laundering network.” Press Release, “United States Files Complaint to Forfeit 280 Cryptocurrency Accounts Tied to Hacks of Two Exchanges by North Korean Actors,” U.S. DEPT. OF JUSTICE (August 27, 2020), available at: <https://www.justice.gov/opa/pr/united-states-files-complaint-forfeit-280-cryptocurrency-accounts-tied-hacks-two-exchanges> (last accessed Oct. 1, 2020). In April 2020, the U.S. Departments of State, Treasury,

and Homeland Security, along with the Federal Bureau of Investigation, issued an advisory on the cyber threat posed by the North Korean regime. The advisory detailed North Korea's use of state-sponsored cyber actors, including "hackers, cryptologists, and software developers," who, among other things, engage in "cyber-enabled theft targeting financial institutions and digital currency exchanges." U.S. DEPT. OF HOMELAND SEC. ET AL., DPRK CYBER THREAT ADVISORY, *Guidance on the North Korean Cyber Threat* (Apr. 15, 2020), available at: https://us-cert.cisa.gov/sites/default/files/2020-04/DPRK_Cyber_Threat_Advisory_04152020_S508C.pdf (last accessed Oct. 1, 2020).

³⁵ Cryptocurrency Crime Losses, *supra* note 33.

³⁶ Press Release, "Operator Of Bitcoin Investment Platform Pleads Guilty To Securities Fraud And Obstruction Of Justice," U.S. DEPT. OF JUSTICE, U.S. ATT'Y'S OFFICE, SDNY (July 23, 2018), available at: <https://www.justice.gov/usao-sdny/pr/operator-bitcoin-investment-platform-pleads-guilty-securities-fraud-and-obstruction> (last accessed Oct. 1, 2020).

³⁷ Press Release, "Trader Sentenced to 15 Months in Federal Prison for Misappropriating \$1.1 Million in Cryptocurrencies," U.S. DEPT. OF JUSTICE, U.S. ATT'Y'S OFFICE, N.D. ILL. (Nov. 13, 2018), available at: <https://www.justice.gov/usao-ndil/pr/trader-sentenced-15-months-federal-prison-misappropriating-11-million-cryptocurrency-0> (last accessed Oct. 1, 2020).

³⁸ Norton, *What is Cryptojacking? How It Works and How to Help Prevent It*, <https://us.norton.com/internetsecurity-malware-what-is-cryptojacking.html> (last accessed Oct. 1, 2020).

³⁹ The aforementioned April 2020 U.S. government advisory regarding North Korea's cyber-hacking program discussed the regime's

potential involvement in multiple cryptojacking schemes. See DPRK CYBER THREAT ADVISORY, *supra* note 34 at 2. Specifically, the advisory noted "several incidents in which computers infected with cryptojacking malware sent the mined assets—much of it anonymity-enhanced digital currency (sometimes also referred to as 'privacy coins')—to servers located in [North Korea]." *Id.* (citing a report by a UN Security Council panel of experts); see also, e.g., Timothy W. Martin, *New North Korea Hack: Hijacking Computers to Power Cryptocurrency Mining*, WALL ST. J., Jan. 8, 2018, available at: https://www.wsj.com/articles/in-north-korea-hackers-mine-cryptocurrency-abroad-1515420004?mod=article_inline (last accessed Oct. 1, 2020).

⁴⁰ Press Release, "Administrators of DeepDotWeb Indicted for Money Laundering Conspiracy, Relating to Kickbacks for Sales of Fentanyl, Heroin and Other Illegal Goods on the Darknet," U.S. DEPT. OF JUSTICE (May 8, 2019), available at: <https://www.justice.gov/opa/pr/administrators-deepdotweb-indicted-money-laundering-conspiracy-relating-kickbacks-sales> (last accessed Oct. 1, 2020). The charges in the indictment are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

⁴¹ See Press Release, "3 Germans Who Allegedly Operated Dark Web Marketplace with Over 1 Million Users Face U.S. Narcotics and Money Laundering Charges," U.S. DEPT. OF JUSTICE, U.S. ATT'Y'S OFFICE, C.D. CAL. (May 3, 2019), available at: <https://www.justice.gov/usao-cdca/pr/3-germans-who-allegedly-operated-dark-web-marketplace-over-1-million-users-face-us> (last accessed Oct. 1, 2020) (describing criminal complaint against the alleged administrators of Wall Street Market (WSM), "one of the world's largest dark web marketplaces that allowed vendors to sell a wide variety of contraband,

including an array of illegal narcotics, counterfeit goods and malicious computer hacking software”).

⁴² Press Release, “J-CODE Announces 61 Arrests in its Second Coordinated Law Enforcement Operation Targeting Opioid Trafficking on the Darknet,” FEDERAL BUREAU OF INVESTIGATION (Mar. 26, 2019), available at: <https://www.fbi.gov/news/pressrel/press-releases/j-code-announces-61-arrests-in-its-second-coordinated-law-enforcement-operation-targeting-opioid-trafficking-on-the-darknet> (last accessed Oct. 1, 2020).

⁴³ Press Release, “International Law Enforcement Operation Targeting Opioid Traffickers on the Darknet Results in over 170 Arrests Worldwide and the Seizure of Weapons, Drugs and over \$6.5 Million,” U.S. DEPT. OF JUSTICE (Sept. 22, 2020), available at: <https://www.justice.gov/opa/pr/international-law-enforcement-operation-targeting-opioid-traffickers-darknet-results-over-170> (last accessed Oct. 1, 2020).

⁴⁴ Press Release, “Administrators of DeepDotWeb Indicted for Money Laundering Conspiracy, Relating to Kickbacks for Sales of Fentanyl, Heroin and Other Illegal Goods on the Darknet,” U.S. DEPT. OF JUSTICE (May 8, 2019), available at: <https://www.justice.gov/opa/pr/administrators-deepdotweb-indicted-money-laundering-conspiracy-relating-kickbacks-sales> (last accessed Oct. 1, 2020). The charges in the indictment are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

⁴⁵ *Id.*

⁴⁶ See 18 U.S.C. §§ 2339A & B.

⁴⁷ See 18 U.S.C. § 792 *et seq.*

⁴⁸ 31 C.F.R. § 1010.100(ff).

⁴⁹ FATF INTERNATIONAL STANDARDS, *supra* note 2, at 127.

⁵⁰ As noted above, “AML/CFT” refers to anti-money laundering and combating the financing of terrorism.

⁵¹ Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1118 (1970). The BSA is the nation’s first and most comprehensive federal AML/CFT statute. The Act, which is codified at 12 U.S.C. § 1829b, 12 U.S.C. §§ 1951–1959, and 31 U.S.C. §§ 5311–5314 and 5316–5332, has been amended at various times, including in October 2001 by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (the “USA PATRIOT Act”). Title III of the USA PATRIOT Act amended the BSA to promote the prevention, detection, and prosecution of international money laundering and the financing of terrorism. Regulations implementing all aspects of the BSA appear at 31 C.F.R. Chapter X.

⁵² The authority of the Secretary of the Treasury to administer the BSA and its implementing regulations has been delegated to the Director of FinCEN. Pursuant to this delegation, FinCEN, among other things, develops AML regulations and enforces compliance with the BSA and associated regulations. See Treas. Order 180-01 (July 1, 2014), available at: <https://www.treasury.gov/about/role-of-treasury/orders-directives/Pages/to180-01.aspx> (last accessed Oct. 1, 2020).

⁵³ See 31 U.S.C. § 310(c); U.S. DEPT. OF THE TREASURY, FIN. CRIMES ENF’T NETWORK, What is the BSA Data?, <https://www.fincen.gov/what-bsa-data> (last accessed Oct. 1, 2020).

⁵⁴ See EGMONT GRP., *Financial Intelligence Units (FIUs)*, <https://egmontgroup.org/en/content/>

[financial-intelligence-units-fius](#) (last accessed Oct. 1, 2020).

⁵⁵ U.S. DEPT. OF THE TREASURY, FIN. CRIMES ENF'T NETWORK, FINCEN GUIDANCE FIN-2019-G001, APPLICATION OF FINCEN'S REGULATIONS TO CERTAIN BUSINESS MODELS INVOLVING CONVERTIBLE VIRTUAL CURRENCIES 7 (May 9, 2019), available at: <https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf> (last accessed Oct. 1, 2020).

⁵⁶ 76 Fed. Reg. 43585 (2011); *see also* 31 CFR § 1010.100(ff)(5)(A) (emphasis added).

⁵⁷ 74 Fed. Reg. 22129, 22137 (2009).

⁵⁸ Press Release, "FinCEN Issues Guidance on Virtual Currencies and Regulatory Responsibilities," U.S. DEPT. OF THE TREASURY, FIN. CRIMES ENF'T NETWORK, (Mar. 18, 2013), available at: <https://www.fincen.gov/news/news-releases/fincen-issues-guidance-virtual-currencies-and-regulatory-responsibilities> (last accessed Oct. 1, 2020).

⁵⁹ *See* FinCEN Guidance FIN-2013-G001, *supra* note 4.

⁶⁰ *Id.*

⁶¹ *See generally* 31 C.F.R. Part 1022 (setting out BSA requirements applicable to MSBs).

⁶² *See* FinCEN Guidance FIN-2019-G001, *supra* note 55.

⁶³ *See id.* at 12.

⁶⁴ *Id.*; *see also* 31 CFR § 1010.100(ff).

⁶⁵ The 2013 FinCEN guidance notes that a virtual currency exchanger is a person engaged as

a business in the exchange of virtual currency for real currency, funds, or other virtual currency. *See* FINCEN GUIDANCE FIN-2013-G001, *supra* note 4, at 2. Further, as noted above, an exchanger is a money transmitter if it accepts and transmits a convertible virtual currency or buys or sells convertible virtual currency for any reason. *Id.* at 3; *see also* Kenneth A. Blanco, Director, U.S. Dept. of the Treasury, Fin. Crimes Enf't Network, Remarks at the 2018 Chicago-Kent Block (Legal) Tech Conference (Aug. 9, 2018), available at: <https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block> (last accessed Oct. 1, 2020).

⁶⁶ *See* 31 U.S.C. § 5321 (authorizing the imposition of civil monetary penalties for violations of the BSA); *see also* 31 C.F.R. §§ 1010.820–821.

⁶⁷ Press Release, "Ripple Labs Inc. Resolves Criminal Investigation," U.S. DEPT. OF JUSTICE (May 5, 2015), available at: <https://www.justice.gov/opa/pr/ripple-labs-inc-resolves-criminal-investigation> (last accessed Oct. 1, 2020); Press Release, "FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger," U.S. DEPT. OF THE TREASURY, FIN. CRIMES ENF'T NETWORK (May 5, 2015), available at: <https://www.fincen.gov/news/news-releases/fincen-fines-ripple-labs-inc-first-civil-enforcement-action-against-virtual> (last accessed Oct. 1, 2020).

⁶⁸ In another example of successful coordination, the Department of Justice in 2017 filed criminal charges against MSB BTC-e and its operator (as discussed above), while FinCEN brought a parallel civil enforcement action. *See* Superseding Indictment, *United States v. BTC-e*, No. CR 16-00227 SI (N.D. Cal. Jan. 17, 2017), available at: <https://www.justice.gov/usao-ndca/press-release/file/984661/download> (last accessed

Oct. 1, 2020); *see also* Press Release, “FinCEN Fines BTC-e Virtual Currency Exchange \$110 Million for Facilitating Ransomware, Dark Net Drug Sales,” U.S. DEPT. OF THE TREASURY, FIN. CRIMES ENF’T NETWORK (July 26, 2017), available at: <https://www.fincen.gov/sites/default/files/2017-07/BTC-e%20July%202026%20Press%20Release%20FINAL1.pdf> (last accessed Oct. 1, 2020).

⁶⁹ *See generally* U.S. DEP’T OF THE TREASURY, *Office of Foreign Assets Control—Sanctions Programs and Information*, <https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx> (last accessed Oct. 1, 2020).

⁷⁰ OFAC uses the term “digital currency,” which includes cryptocurrency and blockchain-based tokens.

⁷¹ U.S. DEP’T OF THE TREASURY, *Resource Center, OFAC FAQs: Sanctions Compliance*, https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx (last accessed Oct. 1, 2020).

⁷² *Id.*

⁷³ *Id.*

⁷⁴ OFAC typically uses Executive Orders to designate persons or entities.

⁷⁵ Press Release, “Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses,” U.S. DEPT. OF THE TREASURY (Nov. 28, 2018), available at: <https://home.treasury.gov/news/press-releases/sm556> (last accessed Oct. 1, 2020). For further discussion of the SamSam ransomware scheme, see *supra* page 8.

⁷⁶ Press Release, “Treasury Designates Iran-Based Financial Facilitators,” *supra* note 75

(“While OFAC routinely provides identifiers for designated persons, today’s action marks the first time OFAC is publicly attributing digital currency addresses to designated individuals. Like traditional identifiers, these digital currency addresses should assist those in the compliance and digital currency communities in identifying transactions and funds that must be blocked and investigating any connections to these addresses.”).

⁷⁷ *Id.*

⁷⁸ Press Release, “Two Iranian Men Indicted,” *supra* note 17; Indictment, *United States v. Savandi et al.*, No. 18-CR-704 (BRM) (D.N.J. Nov. 26, 2018), available at: <https://www.justice.gov/opa/press-release/file/1114741/download> (last accessed Oct. 1, 2020).

⁷⁹ Press Release, “Treasury Targets Chinese Drug Kingpins Fueling America’s Deadly Opioid Crisis,” U.S. DEPT. OF THE TREASURY (Aug. 21, 2019), available at: <https://home.treasury.gov/news/press-releases/sm756> (last accessed Oct. 1, 2020).

⁸⁰ Press Release, “Chinese National Indicted in Southern District of Mississippi Designated by U.S. Treasury Department as Significant Foreign Narcotics Trafficker,” U.S. DEPT. OF JUSTICE (Aug 22, 2019), available at: <https://www.justice.gov/usao-sdms/pr/chinese-national-indicted-southern-district-mississippi-designated-us-treasury> (last accessed Oct. 1, 2020).

⁸¹ Press Release, “Two Chinese Nationals Charged with Operating Global Opioid and Drug Manufacturing Conspiracy Resulting in Deaths,” U.S. DEPT. OF JUSTICE (Aug 22, 2018), available at: <https://www.justice.gov/opa/pr/two-chinese-nationals-charged-operating-global-opioid-and-drug-manufacturing-conspiracy> (last accessed Oct. 1, 2020).

⁸² Press Release, “Treasury Sanctions Russia-Linked Election Interference Actors,” U.S. DEPT. OF THE TREASURY (Sept. 10, 2020), available at: <https://home.treasury.gov/news/press-releases/sm1118> (last accessed Oct. 1, 2020).

⁸³ Press Release, “Russian Project Lakhta Member Charged with Wire Fraud Conspiracy,” U.S. DEPT. OF JUSTICE (Sept. 10, 2020), available at: <https://www.justice.gov/opa/pr/russian-project-lakhta-member-charged-wire-fraud-conspiracy> (last accessed Oct. 1, 2020); see also Indictment, *United States v. Netyksho et al.*, Case No. 18-cr-00215 (D.D.C. 2018), available at: <https://www.justice.gov/file/1080281/download> (alleging Russian intelligence officers’ use of cryptocurrency to launder funds used in furtherance of U.S. election-related hacking activity) (last accessed Oct. 1, 2020).

⁸⁴ See *supra* note 32 and accompanying text.

⁸⁵ Press Release, “Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group,” U.S. DEPT. OF THE TREASURY (Mar. 2, 2020), available at: <https://home.treasury.gov/news/press-releases/sm924> (last accessed Oct. 1, 2020).

⁸⁶ Press Release, “Two Chinese Nationals Charged with Laundering Over \$100 Million in Cryptocurrency From Exchange Hack,” U.S. DEPT. OF JUSTICE (Mar. 2, 2020), available at: <https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack> (last accessed Oct. 1, 2020); Indictment, *United States v. Yinyin*, No. 1:20-cr-00052-TJK (D.D.C. Feb. 27, 2020), available at: <https://www.justice.gov/opa/press-release/file/1253486/download> (last accessed Oct. 1, 2020) (charging two Chinese nationals with conspiracy to launder monetary instruments under 18 U.S.C. § 1956(h) and operating an unlicensed money transmitted business under 18 U.S.C. § 1960(a), and seeking forfeiture under 18

U.S.C. § 982(a)(1) and 21 U.S.C. § 853(p)). The charges in the indictment are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

⁸⁷ Press Release, “United States Files Complaint to Forfeit 280 Cryptocurrency Accounts,” *supra* note 34.

⁸⁸ Press Release, “Two Chinese Nationals Charged with Laundering Over \$100 Million,” *supra* note 86.

⁸⁹ Press Release, “United States Files Complaint to Forfeit 280 Cryptocurrency Accounts,” *supra* note 34.

⁹⁰ Verified Complaint, *United States v. 280 Virtual Currency Accounts*, Civ. No. 20-2396, at 11–12 (D.D.C. Aug. 27, 2020), available at: <https://www.justice.gov/opa/press-release/file/1310421/download> (last accessed Oct. 1, 2020).

⁹¹ Verified Complaint, *United States v. 113 Virtual Currency Accounts*, Civ. No. 20-606, at 4 (D.D.C. Mar. 2, 2020), available at: <https://www.justice.gov/opa/press-release/file/1253491/download> (last accessed Oct. 1, 2020).

⁹² *Id.* at 5.

⁹³ OFFICE OF THE COMPTROLLER OF THE CURRENCY, *What We Do*, <https://www.occ.treas.gov/about/index-about.html> (last accessed Oct. 1, 2020).

⁹⁴ OCC Interpretative Letter #1170, *Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers* (July 22, 2020), available at: <https://www.occ.treas.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf> (last accessed Oct. 1, 2020).

⁹⁵ *Id.* at 1.

⁹⁶ *Id.* Shortly before this Enforcement Framework was finalized for publication, OCC on September 21, 2020 published an interpretive letter clarifying national banks' and federal savings associations' authority—in certain defined circumstances—to hold “reserves” on behalf of customers who issue certain “stablecoins.” (“Stablecoins” are a type of cryptocurrency designed to have a stable value as compared with other types of cryptocurrency, which frequently experience significant volatility.) OCC’s Sept. 21 letter represents the latest step in the agency’s broader effort to set up systems that will enable banks to adopt cryptocurrency safely. The interpretive letter is available at <https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1172.pdf> (last accessed Oct. 1, 2020).

⁹⁷ See OCC Consent Order, In re *M.Y. Safra Bank, FSB*, AA-NE-2020-5, at 3 (Jan. 30, 2020), available at: <https://www.occ.gov/static/enforcement-actions/ea2020-005.pdf> (last accessed Oct. 1, 2020).

⁹⁸ U.S. SEC. AND EXCH. COMM’N, RELEASE NO. 81207: REPORT OF INVESTIGATION PURSUANT TO SECTION 21(A) OF THE SECURITIES EXCHANGE ACT OF 1934: THE DAO 10 (July 25, 2017), available at: <https://www.sec.gov/litigation/investreport/34-81207.pdf> (last accessed Oct. 1, 2020).

⁹⁹ U.S. SEC. & EXCH. COMM’N STAFF, FRAMEWORK FOR ‘INVESTMENT CONTRACT’ ANALYSIS OF DIGITAL ASSETS, available at: <https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets> (last accessed Oct. 1, 2020); FINANCIAL INDUSTRY REGULATORY AUTHORITY, *Initial Coin Offerings*, <https://www.finra.org/investors/learn-to-invest/types-investments/initial-coin-offerings-and-cryptocurrencies/initial-coin-offerings> (last accessed Oct. 1, 2020).

¹⁰⁰ The Financial Industry Regulatory Authority (FINRA), which operates under the supervision of the SEC, has issued several investor alerts regarding key cryptocurrency issues, such as ICOs and cryptocurrency-related scams. See, e.g., FINANCIAL INDUSTRY REGULATORY AUTHORITY, *Investor Alert, Initial Coin Offerings (ICOs)—What to Know Now and Time-Tested Tips for Investors*, <https://www.finra.org/investors/alerts/icos-what-know-now> (last accessed Oct. 1, 2020); FINANCIAL INDUSTRY REGULATORY AUTHORITY, *Investor Alert, Don’t Fall for Cryptocurrency-Related Stock Scams*, <https://www.finra.org/investors/alerts/cryptocurrency-related-stock-scams> (last accessed Oct. 1, 2020).

¹⁰¹ SEC RELEASE NO. 81207, *supra* note 98.

¹⁰² *Id.* at 17–18; see also Jay Clayton [SEC Chairman] and Christopher Giancarlo [CFTC Chairman], *Regulators are Looking at Cryptocurrency*, WALL ST. J., Jan. 24, 2018, available at: <https://www.wsj.com/articles/regulators-are-looking-at-cryptocurrency-1516836363> (“The SEC does not have direct oversight of transactions in currencies or commodities. Yet some products that are labeled cryptocurrencies have characteristics that make them securities. The offer, sale and trading of such products must be carried out in compliance with securities law.”) (last accessed Oct. 1, 2020).

¹⁰³ Section 12(k)(1) of the Securities Exchange Act provides the SEC with authority “summarily to suspend trading in any security,” other than certain exempted securities, “for a period not exceeding 10 business days” if doing so is, in the SEC’s opinion, “in the public interest” and required for “the protection of investors.” 15 U.S.C. § 78l(k)(1).

¹⁰⁴ The SEC Staff publishes a list of its digital-asset- and ICO-related enforcement actions on its website. See U.S. SEC. AND EXCH. COMM’N, *Cyber Enforcement Actions*, <https://www.sec.gov/spotlight/cybersecurity-enforcement-actions> (last accessed Oct. 1, 2020); see also U.S. SEC. & EXCH. COMM’N, *Spotlight on Initial Coin Offerings and Digital Assets*, <https://www.investor.gov/additional-resources/spotlight/spotlight-initial-coin-offerings-and-digital-assets> (collecting SEC resources on ICOs and other digital-asset-related issues) (last accessed Oct. 1, 2020).

¹⁰⁵ FRAMEWORK FOR ‘INVESTMENT CONTRACT’ ANALYSIS OF DIGITAL ASSETS, *supra* note 99.

¹⁰⁶ *SEC v. W. J. Howey Co.*, 328 U.S. 293, 301 (1946).

¹⁰⁷ FRAMEWORK FOR ‘INVESTMENT CONTRACT’ ANALYSIS OF DIGITAL ASSETS, *supra* note 99.

¹⁰⁸ The public can engage with SEC Staff through the SEC’s Strategic Hub for Innovation and Financial Technology (FinHub). U.S. SEC. AND EXCH. COMM’N, *FinHub*, www.sec.gov/finhub (last accessed Oct. 1, 2020).

¹⁰⁹ Press Release, “SEC Halts Alleged \$1.7 Billion Unregistered Digital Token Offering,” U.S. SEC. AND EXCH. COMM’N (Oct. 11, 2019), available at: <https://www.sec.gov/news/press-release/2019-212> (last accessed Oct. 1, 2020).

¹¹⁰ *Id.*

¹¹¹ *Id.*

¹¹² *Id.* In response, Telegram and TON Issuer argued that the sale of Grams to sophisticated investors were lawful private placements of securities covered by an exemption from the

registration requirement, and that the anticipated resale of the Grams by those investors to a secondary public market, upon the launch of the TON Blockchain, were unrelated transactions that would not amount to the offer or sale of securities. See *SEC v. Telegram Group Inc.*, No. 19-cv-09439-PKC, 2020 WL 1430035, at *1 (S.D.N.Y. Mar. 24, 2020).

¹¹³ *Id.*

¹¹⁴ *Id.*

¹¹⁵ Final Judgment, *SEC v. Telegram Group Inc.*, No. 19-cv-09439-PKC, (S.D.N.Y. June 26, 2020), Dkt. No. 242.

¹¹⁶ For example, in April 2019, the SEC’s Division of Corporation Finance provided a “no-action letter” in response to an inquiry from TurnKey Jet, Inc., an interstate air charter services company that proposed “to offer and sell blockchain-based digital assets in the form of ‘tokenized’ jet cards” without registering under the Securities Act of 1933 or the Securities Exchange Act of 1934. See Letter from James P. Curry to SEC Office of Chief Counsel (Apr. 2, 2019), available at: <https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1-incoming.pdf> (last accessed Oct. 1, 2020). The no-action letter stated that the Division of Corporation Finance would not recommend enforcement action against the company if, based on the facts presented, it offered and sold tokens without registration. See TurnKey Jet, Inc., SEC No-Action Letter (Apr. 3, 2019), available at: <https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm> (last accessed Oct. 1, 2020).

¹¹⁷ For examples of prosecutions for securities and other fraud relating to ICOs, see, for example, Press Release, “Brooklyn Businessman Pleads Guilty to

Defrauding Investors through Two Initial Coin Offerings,” U.S. DEPT. OF JUSTICE, U.S. ATT’Y’S OFFICE, E.D.N.Y. (Nov. 15, 2018) (discussing *United States v. Zaslavskiy*, No. 17 CR 647 (RJD) (E.D.N.Y. 2018)), available at: <https://www.justice.gov/usao-edny/pr/brooklyn-businessman-pleads-guilty-defrauding-investors-through-two-initial-coin> (last accessed Oct. 1, 2020), and Press Release, “Founders Of Cryptocurrency Company Indicted In Manhattan Federal Court With Scheme To Defraud Investors,” U.S. DEPT. OF JUSTICE, U.S. ATT’Y’S OFFICE, S.D.N.Y. (May 14, 2018), (discussing *United States v. Sharma, et. al.*, No. 18 Cr. 340 (LGS) (S.D.N.Y. 2019)), available at: <https://www.justice.gov/usao-sdny/pr/founders-cryptocurrency-company-indicted-manhattan-federal-court-scheme-defraud> (last accessed Oct. 1, 2020).

¹¹⁸ Press Release, “SEC Halts Alleged Initial Coin Offering Scam,” U.S. SEC. AND EXCH. COMM’N (Jan. 30, 2018), available at: <https://www.sec.gov/news/press-release/2018-8> (last accessed Oct. 1, 2020).

¹¹⁹ Press Release, “Cryptocurrency CEO Indicted After Defrauding Investors of \$4 Million,” U.S. DEPT. OF JUSTICE, U.S. ATT’Y’S OFFICE, N.D. TEX. (Nov. 28, 2018), available at: <https://www.justice.gov/usao-ndtx/pr/cryptocurrency-ceo-indicted-after-defrauding-investors-4-million> (last accessed Oct. 1, 2020); Indictment, *United States v. Rice*, No. 3:18-CR-587-K (N.D. Tex. Nov. 20, 2018), available at: <https://www.justice.gov/usao-ndtx/press-release/file/1115456/download> (last accessed Oct. 1, 2020).

¹²⁰ Press Release, “Executives Settle ICO Scam Charges,” U.S. SEC. AND EXCH. COMM’N (Dec. 12, 2018), available at: <https://www.sec.gov/news/press-release/2018-280> (last accessed Oct. 1, 2020).

¹²¹ 7 U.S.C. § 1 *et seq.*

¹²² These terms are defined in the CFTC’s Glossary. See U.S. COMMODITY FUTURES TRADING COMM’N, *CFTC Glossary*, <https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/CFTCGlossary/index.htm> (last accessed Oct. 1, 2020).

¹²³ 7 U.S.C. § 1(a)(9).

¹²⁴ See *In re Kim*, CFTC No. 19-02, 2018 WL 5993718, at *3 (Oct. 29, 2018) (consent order) (“Virtual currencies such as Bitcoin and Litecoin are encompassed in the definition of ‘commodity’ under [the CEA].”); *In re Coinflip, Inc.*, CFTC No. 15-29, 2015 WL 5535736, at *2 (Sept. 17, 2015) (consent order) (“Bitcoin and other virtual currencies are encompassed in the definition and properly defined as commodities.”); *In re TeraExchange LLC*, CFTC No. 15-33, 2015 WL 5658082, at *3 n.3 (Sept. 24, 2015) (consent order) (“Further, bitcoin is a commodity under Section 1a of the Act, 7 U.S.C. § 1a (2012), and is therefore subject as a commodity to applicable provisions of the [CEA] and [CFTC] Regulations.”).

¹²⁵ See *CFTC v. McDonnell*, 287 F. Supp. 3d 213, 217 (E.D.N.Y. 2018) (“Virtual currencies can be regulated by CFTC as a commodity. . . . They fall well-within the common definition of ‘commodity’ as well as the [CEA’s] definition of ‘commodities’ as ‘all other goods and articles . . . in which contracts for future delivery are presently or in the future dealt in.’”); *CFTC v. My Big Coin Pay, Inc.*, 334 F. Supp. 3d 492, 495–98 (D. Mass. 2018) (applying a categorical approach to interpreting “commodity” under the CEA and determining that a non-bitcoin virtual currency is a “commodity” under the Act).

¹²⁶ U.S. COMMODITY FUTURES TRADING COMM’N, A CFTC PRIMER ON VIRTUAL CURRENCIES 11 (Oct. 2017), available at: https://www.cftc.gov/sites/default/files/idc/groups/public/documents/file/labcftc_primercurrencies100417.pdf (last accessed Oct. 1, 2020).

¹²⁷ See, e.g., *In re Plutus Financial Inc.*, CFTC No. 20-23, 2020 WL 4043709 (July 13, 2020) (consent order); *In re BitFinex Inc.*, CFTC No. 16-19, 2016 WL 3137612 (June 2, 2016) (consent order); *In re Coinflip, Inc.*, CFTC No. 15-29, 2015 WL 5535736 (Sept. 17, 2015) (consent order).

¹²⁸ *In re TeraExchange*, CFTC No. 15-33, 2015 WL 5658082 (Sept. 24, 2015) (consent order).

¹²⁹ *CFTC v. 1Pool Ltd.*, No. 1:18-cv-2243-TNM, 2019 WL 1605201 (Mar. 4, 2019).

¹³⁰ Retail Commodity Transactions Involving Certain Digital Assets, 85 Fed. Reg. 37734 (June 24, 2020) (to be codified at 17 C.F.R. pt. 1).

¹³¹ Press Release, “CFTC Staff Issues Advisory for Virtual Currency Products,” COMMODITY FUTURES TRADING COMM’N (May 21, 2018), available at <https://www.cftc.gov/PressRoom/PressReleases/7731-18> (last accessed Oct. 1, 2020).

¹³² See, e.g., *CFTC v. McDonnell*, 287 F. Supp. 3d 213, 217 (E.D.N.Y. 2018); *CFTC v. My Big Coin Pay, Inc.*, 334 F. Supp. 3d 492, 495–98 (D. Mass. 2018).

¹³³ Press Release, “CFTC Charges Multiple Individuals and Companies with Operating a Fraudulent Scheme Involving Binary Options and a Virtual Currency Known as ATM Coin,” COMMODITY FUTURES TRADING COMM’N (Apr. 18, 2018), available at: <https://www.cftc.gov/PressRoom/PressReleases/7714-18> (last accessed Oct. 1, 2020).

¹³⁴ Press Release, “Federal Court Orders Defendants to Pay More than \$4.25 Million for Fraud and Misappropriation,” COMMODITY FUTURES TRADING COMM’N (Nov. 1, 2019), available at: <https://www.cftc.gov/PressRoom/>

[PressReleases/8069-19](https://www.cftc.gov/PressRoom/PressReleases/8069-19) (last accessed Oct. 1, 2020).

¹³⁵ See Indictment, *United States v. Kantor*, No. 18-CR-177 (E.D.N.Y. Apr. 10, 2018), available at: <https://www.justice.gov/usao-edny/press-release/file/1053266/download> (last accessed Oct. 1, 2020); Press Release, “Defendant Sentenced to 86 Months in Prison for Defrauding Investors in Binary Options and Cryptocurrency Scheme,” U.S. DEPT. OF JUSTICE, U.S. ATT’Y’S OFFICE, E.D.N.Y. (July 1, 2019), available at: <https://www.justice.gov/usao-edny/pr/defendant-sentenced-86-months-prison-defrauding-investors-binary-options-and> (last accessed Oct. 1, 2020).

¹³⁶ Notice 2014-21, 2014-16 I.R.B. 938, available at: <https://www.irs.gov/pub/irs-drop/n-14-21.pdf> (last accessed Oct. 1, 2020).

¹³⁷ Since July 2019, the IRS has sent thousands of warning letters to taxpayers “that potentially failed to report income and pay the resulting tax from virtual currency transactions or did not report their transactions properly.” News Release, “IRS has Begun Sending Letters to Virtual Currency Owners Advising Them to Pay Back Taxes, File Amended Returns; Part of Agency’s Larger Efforts,” INTERNAL REVENUE SERV. (July 26, 2019), available at: <https://www.irs.gov/newsroom/irs-has-begun-sending-letters-to-virtual-currency-owners-advising-them-to-pay-back-taxes-file-amended-returns-part-of-agencys-larger-efforts> (last accessed Oct. 1, 2020).

¹³⁸ “A John Doe summons is a summons that does not identify the person with respect to whose liability the summons is issued.” INTERNAL REVENUE MANUAL, Part 25.5.7, *Special Procedures for John Doe Summonses*, available at: https://www.irs.gov/irm/part25/irm_25-005-007 (last accessed Oct. 1, 2020). The IRS can use John

Doe summonses, which require court approval, in certain circumstances “to obtain information about possible violations of internal revenue laws by individuals whose identities are unknown.” Press Release, “Court Authorizes Service of John Doe Summons Seeking the Identities of U.S. Taxpayers Who Have Used Virtual Currency,” U.S. DEPT. OF JUSTICE (Nov. 30, 2016), available at: <https://www.justice.gov/opa/pr/court-authorizes-service-john-doe-summons-seeking-identities-us-taxpayers-who-have-used> (last accessed Oct. 1, 2020).

¹³⁹ Rev. Rul. 2019-24, 2019-44 I.R.B. 1004, available at: <https://www.irs.gov/pub/irs-drop/rr-19-24.pdf> (last accessed Oct. 1, 2020).

¹⁴⁰ INTERNAL REVENUE SERV., Frequently Asked Questions on Virtual Currency Transactions, <https://www.irs.gov/individuals/international-taxpayers/frequently-asked-questions-on-virtual-currency-transactions> (last accessed Oct. 1, 2020).

¹⁴¹ *Id.*

¹⁴² N. AM. SEC. ADM’RS ASS’N, *Our Role*, <http://www.nasaa.org/about-us/our-role/> (last accessed Oct. 1, 2020).

¹⁴³ NASAA, which is comprised of State and territorial securities regulators, has taken an active role in investor education and in coordinating State actions involving VASPs and ICOs. *See, e.g.*, N. AM. SEC. ADM’RS ASS’N, INFORMED INVESTOR ADVISORY: INITIAL COIN OFFERINGS (Apr. 2018), available at <https://www.nasaa.org/44836/informed-investor-advisory-initial-coin-offerings/?qoid=investor-education> (last accessed Oct. 1, 2020).

¹⁴⁴ News Release, “State and Provincial Securities Regulators Conduct Coordinated International Crypto Crackdown,” N. AM. SEC. ADM’RS ASS’N (May 21, 2018), available at: <http://www.nasaa.org/45121/state-and-provincial-securities-regulators-conduct-coordinated-international-crypto-crackdown-2/> (last accessed Oct. 1, 2020).

¹⁴⁵ *See* N.Y. STATE OFFICE OF THE ATT’Y GEN., VIRTUAL MARKETS INTEGRITY INITIATIVE REPORT (Sept. 18, 2018), available at: <https://virtualmarkets.ag.ny.gov/> (last accessed Oct. 1, 2020).

¹⁴⁶ Press Release, “A.G. Schneiderman Launches Inquiry into Cryptocurrency ‘Exchanges,’” N.Y. STATE OFFICE OF THE ATT’Y GEN. (Apr. 17 2018), available at: <https://ag.ny.gov/press-release/ag-schneiderman-launches-inquiry-cryptocurrency-exchanges> (last accessed Oct. 1, 2020).

¹⁴⁷ The FATF is also known by its French name, Groupe d’action financière (or “GAFI”).

¹⁴⁸ FINANCIAL ACTION TASK FORCE, *What Do We Do*, <http://www.fatf-gafi.org/about/whatwedo/> (last accessed Oct. 1, 2020).

¹⁴⁹ FATF INTERNATIONAL STANDARDS, *supra* note 2, Recommendation 15.

¹⁵⁰ *See id.* at 70–71.

¹⁵¹ The FATF has undertaken a 12-month review and committed further to a 24-month review of countries’ progress with implementing the revised requirements for VASPs. The FATF’s 12-month review concluded that there has been progress in implementation of the standards, but that much more remains to be done globally by individual jurisdictions. The report further determined that, while there is no need to revise the standards, there is a need for updated guidance, which the FATF plans to release in 2021. The FATF also undertook a report on so-called “stablecoins” at the request of the G20. This report also found no need to update the FATF standards, but did identify a number of concerns that will be addressed in forthcoming guidance.

¹⁵² See 31 C.F.R. §§ 1010.100(ff), 1022.380; *see also* U.S. DEPT. OF THE TREASURY, FIN. CRIMES ENF'T NETWORK, FINCEN ADVISORY FIN-2012-A001: FOREIGN-LOCATED MONEY SERVICES BUSINESSES (Feb. 2012), available at: <https://www.fincen.gov/sites/default/files/advisory/FIN-2012-A001.pdf> (last accessed Oct. 1, 2020); U.S. DEPT. OF THE TREASURY, FIN. CRIMES ENF'T NETWORK, *Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses*, 76 F.R. 43585 (July 21, 2011), available at <http://www.gpo.gov/fdsys/pkg/FR-2011-07-21/pdf/2011-18309.pdf> (last accessed Oct. 1, 2020).

¹⁵³ Many P2P exchange platforms also offer wallet and escrow services, advertising for buyers and sellers, and messaging or chat functions. Generally, platforms that offer hosted wallet services also are MSBs and must comply with the relevant regulations.

¹⁵⁴ See 31 U.S.C. §§ 5318 & 5322.

¹⁵⁵ See *supra* Part I at page 14 (discussing KYC requirements).

¹⁵⁶ Press Release, “O.C. Man Admits Operating Unlicensed ATM Network that Laundered Millions of Dollars of Bitcoin and Cash for Criminals’ Benefit,” U.S. DEPT. OF JUSTICE, U.S. ATT’Y’S OFFICE, C.D. CAL. (July 22, 2020), available at: <https://www.justice.gov/usao-cdca/pr/oc-man-admits-operating-unlicensed-atm-network-laundered-millions-dollars-bitcoin-and> (last accessed Oct. 1, 2020).

¹⁵⁷ 31 C.F.R. 1010.100(t)(5)(i).

¹⁵⁸ See Press Release, “Ohio Resident Charged with Operating Darknet-Based Bitcoin ‘Mixer,’ which Laundered Over \$300 Million,” U.S. DEPT. OF JUSTICE (Feb. 13, 2020), available at: <https://>

www.justice.gov/opa/pr/ohio-resident-charged-operating-darknet-based-bitcoin-mixer-which-laundered-over-300-million (last accessed Oct. 1, 2020). The charges in the indictment are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

¹⁵⁹ 18 U.S.C. § 1956(a)(1)(B)(i).

¹⁶⁰ Verified Complaint, *United States v. 280 Virtual Currency Accounts*, *supra* note 90, at 11.

¹⁶¹ Last year, the Law Library of Congress published a comprehensive report on over 40 international jurisdictions’ regulatory approaches to cryptoassets, focusing on those jurisdictions’ financial market and investor protection laws, as well as on their application of tax and AML/CFT laws. That report confirms the vast diversity of domestic virtual currency regulation, and practice, across the globe. See LAW LIBRARY OF CONGRESS, *Regulatory Approaches to Cryptoassets in Selected Jurisdictions* (April 2019), available at: <https://www.loc.gov/law/help/cryptoassets/cryptoasset-regulation.pdf> (last accessed Oct. 1, 2020).

¹⁶² See, e.g., *United States v. Lord*, 915 F.3d 1009 (5th Cir. 2019); *United States v. Stetkiw*, No. 18-20579, 2019 WL 417404 (E.D. Mich. Feb. 1, 2019); *United States v. Tetley*, No. 17-cr-00738 (C.D. Cal. 2018); *United States v. Mansy*, No. 2:15-cr-198-GZS, 2017 WL 9672554 (D. Maine May 11, 2017); *United States v. Petix*, No. 15-CR-227A, 2016 WL 7017919 (W.D.N.Y. Dec. 1, 2016); *United States v. Noland et al.*, 14-cr-00401-RM (D. Col. 2015); see also Press Release, “Bitcoin Maven’ Sentenced to One Year,” *supra* note 23.

¹⁶³ *United States v. Al Kassar*, 660 F.3d 108, 118 (2d Cir. 2011) (citing *United States v. Peterson*, 812 F.2d 486, 494 (9th Cir. 1987)).

¹⁶⁴ For more on the concept of protective jurisdiction in the context of U.S. material support statutes, see John De Pue, *Extraterritorial Jurisdiction and the Material Support Statutes*, U.S. ATTY'S BULLETIN, Sept. 2014, available at: <https://www.justice.gov/sites/default/files/usao/legacy/2014/09/23/usab6205.pdf> (last accessed Oct. 1, 2020).

¹⁶⁵ See *supra* Part I at page 14.

¹⁶⁶ See *supra* Part I at 18, 19.

¹⁶⁷ Verified Complaint for Forfeiture *In Rem, United States v. Cazes*, No. 1:17-at-00557, at 21 (E.D. Cal. July 19, 2017), available at: <https://www.justice.gov/opa/press-release/file/982821/download> (last accessed Oct. 1, 2020).

¹⁶⁸ Press Release, "AlphaBay, the Largest Online 'Dark Market,' Shut Down," U.S. DEPT. OF JUSTICE (July 20, 2017), available at: <https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down> (last accessed Oct. 1, 2020).

¹⁶⁹ These criminal charges included: narcotics conspiracy (21 U.S.C. §§ 846 and 841(a)(1), (b)(1)(A), (b)(1)(C), 841(h), and 843(b)); distribution of a controlled substance (21 U.S.C. §§ 841(a)(1), (b)(1)(C), & 846); conspiracy to commit identity theft and fraud (18 U.S.C. § 1028(f)); unlawful transfer of a false identification document (18 U.S.C. § 1028(a)(2), (b)(1)(A)(ii), & (f)); conspiracy to commit access device fraud (18 U.S.C. § 1029(b)(2)); trafficking in device making equipment (18 U.S.C. § 1029(a)(4), (b)(1), & (c)(1)(A)(ii)); and money laundering conspiracy (18 U.S.C. § 1956(h)). See Indictment, *United States v. Cazes*, Case No. 1:17-CR-00144 (E.D. Cal. June 1, 2017), available at: <https://www.justice.gov/opa/press-release/file/982826/download> (last accessed Oct. 1, 2020). In addition, prosecutors used various

criminal forfeiture statutes (18 U.S.C. §§ 982(a)(1) and 982(a)(2)(B) and 21 U.S.C. § 853(a)). *Id.*

¹⁷⁰ Verified Complaint, *United States v. 280 Virtual Currency Accounts*, *supra* note 90, at 11.

¹⁷¹ U.S. DEPT. OF JUSTICE, REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE 100-01 (July 2018), available at: <https://www.justice.gov/cyberreport> (last accessed Oct. 1, 2020).

¹⁷² *Id.* at 101.

¹⁷³ Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 6.1(c) & (f), available at <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32016R0679> (last accessed Oct. 1, 2020).

¹⁷⁴ *Id.*, art. 49.1 & 49.1(d).

¹⁷⁵ Br. of the European Comm'n on Behalf of the E.U. as Amicus Curiae in Support of Neither Party, *United States v. Microsoft*, No. 17-2 (U.S. 2018), available at: https://www.supremecourt.gov/tPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf (last accessed Oct. 1, 2020).

¹⁷⁶ *Id.* at 15.

¹⁷⁷ General Data Protection Regulation, art. 49.1(e), *supra* note 173