FINTECH

NOTES

Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (2)

Effective Anti-Money Laundering and Combating the Financing of Terrorism Regulatory and Supervisory Framework—Some Legal and Practical Considerations

Nadine Schwarz, Ke Chen, Kristel Poh, Grace Jackson, Kathleen Kao, Francisca Fernando, and Maksym Markevych

NOTE/2021/003

FINTECH NOTE

Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (2)

Effective Anti-Money Laundering and Combating the Financing of Terrorism Regulatory and Supervisory Framework—Some Legal and Practical Considerations

Prepared by Nadine Schwarz, Ke Chen, Kristel Poh, Grace Jackson, Kathleen Kao, Francisca Fernando, and Maksym Markevych

October 2021

INTERNATIONAL MONETARY FUND

Cover Design: IMF Creative Services
Composition: The Grauel Group

Names: Schwarz, Nadine. | Chen, Ke (Financial Sector Expert). | Poh, Kristel. | Jackson, Grace. | Kao, Kathleen. | Fernando, Francisca. | Markevych, Maksym. | International Monetary Fund, publisher.
Title: Virtual assets and anti-money laundering and combating the financing of terrorism (2): effective anti-money laundering and combating the financing of terrorism regulatory and supervisory framework—some legal and practical considerations / prepared by Nadine Schwarz, Ke Chen, Kristel Poh, Grace Jackson, Kathleen Kao, Francisca Fernando, and Maksym Markevych.
Other titles: FinTech notes (International Monetary Fund).
Description: Washington, DC : International Monetary Fund, 2021. | October 2021. | Fintech notes | Includes bibliographical references.
Identifiers: ISBN 9781513593821 (paper)
Subjects: LCSH: Money laundering—Prevention—Law and legislation. | Terrorism—Prevention—Law and legislation. | Digital currency—Law and legislation.
Classification: LCC HV6768.S393 2021

Publication orders may be placed online, by fax, or through the mail:
International Monetary Fund, Publication Services
PO Box 92780, Washington, DC 20090, U.S.A.
Tel.: (202) 623-7430 Fax: (202) 623-7201
Email: publications@imf.org
www.imf bookstore.org

CONTENTS

ABBREVIATIONS

AI	Artificial Intelligence
AML/CFT	Anti-Money Laundering/Combating the Financing of Terrorism
CDD	Customer Due Diligence
Digital ID	Digital Identification
DLT	Distributed Ledger Technology
DNFBPs	Designated Non-Financial Businesses and Professions
FATF	Financial Action Task Force
FI	Financial Institution
FIU	Financial Intelligence Unit
ML	Money Laundering
PEP	Politically Exposed Person
PF	Financing of Proliferation of Weapons of Mass Destruction
STR	Suspicious Transaction Report
TF	Terrorist Financing
UNSC	United Nations Security Council
VA	Virtual Asset
VASP	Virtual Asset Service Provider

VIRTUAL ASSETS AND ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (2): EFFECTIVE AML/CFT REGULATORY AND SUPERVISORY FRAMEWORK—SOME LEGAL AND PRACTICAL CONSIDERATIONS

Introduction

Financial technology presents enormous opportunities as well as potentially significant risks to the integrity of the financial system. This is particularly the case with virtual assets (VAs), a broad term describing systems of storing/capturing value in digital form—that includes what are referred to as "digital currencies," "cryptocurrencies," and other terminologies, including existing stablecoins and so-called global stablecoins[1] currently being developed. Enabling the greater speed, lower cost, and increased efficiency in making payments and transfers, including across borders, they have the potential to improve financial inclusion. While generally used for legitimate purposes, some VAs have been misused to commit narcotic-related crimes, fraud, theft, money laundering (ML), and terrorist financing (TF), among other illegal activities.[2] The mitigation of these financial integrity risks requires careful consideration and effective implementation of the Financial Action Task Force (FATF) anti–money laundering/combating the financing of terrorism (AML/CFT) standards.[3]

To assist its member jurisdictions to understand and mitigate the financial integrity risks posed by VAs, IMF staff has prepared two Fintech Notes devoted to VAs and AML/CFT. The first note[4] explains why VAs are vulnerable to misuse for ML/TF/financing of proliferation of weapons of mass destruction (PF) purposes and clarifies which assets and service providers should be subject to AML/CFT measures, the measures that all jurisdictions should take, and the type of action necessary in instances of criminal misuse of VA.

This second Fintech note focuses on the AML/CFT regulation and supervision of VASPs. It builds upon Fintech Note 1 and is aimed at providing policy makers as well as competent authorities with a high-level overview of the AML/CFT regulatory and supervisory frameworks envisaged for VA and VASPs and of some of the legal and practical considerations that they raise.[5] While countries may opt to restrict VA activities within their jurisdiction (e.g., by banning transactions in VA or banning certain types of VAs or even certain VA-related activities), this option is likely to become increasingly challenging as VAs gain greater portions of the financial markets. Many jurisdictions choose to ride the virtual wave and reap the benefits of VAs while mitigating the risks by making VASPs part of the mitigation solution. This requires the implementation of measures built on top of those explained in the Fintech Note 1 (e.g., ensuring appropriate coverage in the ML and TF offenses), such as licensing or registration of VASPs, imposing AML/CFT obligations on VASPs and monitoring compliance with these obligations. These measures are equivalent to those already imposed on financial institutions and designated nonfinancial

The views expressed in this note are those of the authors and do not necessarily represent the views of the IMF, its Executive Board, or its management. The authors are grateful to Yan Liu for her support and guidance, and to Nadim Kyriakos-Saad, Trevor Rajah, Wouter Bossu, Steve Dawe, Christophe Waerzeggers, Arthur Rossi, Kohei Noda, Jane Duasing for their review and comments. This note also greatly benefited from comments from colleagues in other IMF departments and staff of the FATF Secretariat.

[1]The Financial Action Task Force (FATF) definition of VAs is included in the Glossary at the end of this note. In a recent paper on this topic, the Financial Stability Board defines stablecoin as a crypto asset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets. Global stablecoin is defined as a stablecoin with a potential reach and adoption across multiple jurisdictions and the potential to achieve substantial volume. Similarly, the FATF noted that "global stablecoins" refers to stablecoins with the potential for mass adoption proposed by some big tech companies. It should also be noted that the FATF definition of VA does not include Central Bank Digital Currencies. The latter are therefore not covered in this note.

[2]See: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html. Some known cases of misuse can be found in "Virtual Assets - Red Flag Indicators" published by the FATF.

[3]The FATF is an intergovernmental body established in 1989 to set standards and promote effective implementation of legal, regulatory, supervisory, and operational measures for combating ML as well as, subsequently, TF and PF. It comprises 39 members representing most major financial centers in the world. See www.fatf-gafi.org.

[4]"Virtual Assets and Anti–Money Laundering and Combating the Financing of Terrorism (AML/CFT)— Some Legal and Practical Considerations".

[5]The IMF Fintech Note, "Regulation of Crypto Assets," discusses some issues pertaining the broader regulatory framework for VAs and VASPs.

businesses and professions (DNFBPs) as defined by the FATF, with some adjustments for the virtual context.

The purpose of this note is to discuss the necessary AML/CFT measures and provide examples of practical solutions to implement them. In June 2020, the FATF noted that both the public and private sectors have made progress in the implementation of VA standards, particularly through updates to national laws and the development of solutions to assist with the travel rule. However, challenges remain. Many VASPs are only beginning to adopt the required AML/CFT measures, a number of jurisdictions are yet to implement the standards for VAs, and those that have are at the early stages of developing a supervisory regime for VASPs.[6] At the time of drafting, no country had been assessed against the new standards and many country authorities were in the process of establishing how best to incorporate the new standards in their AML/CFT framework. For these reasons, this note does not refer to specific country examples. References to specific products and projects are made for illustrative purposes only and do not constitute an endorsement of these initiatives. This note, like the one on "Virtual Assets and Anti–Money Laundering and Combating the Financing of Terrorism (AML/CFT)— Some Legal and Practical Considerations," is based on the FATF standards and guidance, particularly those aspects that pertain to VAs and VASPs.[7]

Effective Regulatory and Supervisory AML/CFT System—Legal and Practical Considerations

As with any other financial business, a strong regulatory and supervisory framework is key to the soundness of the VASP industry. As a starting point, jurisdictions should ensure that all VASPs are properly licensed or registered and subject to adequate AML/CFT obligations. They should then ensure that VASPs are adequately supervised for AML/CFT purposes and that unauthorized VASPs and failure to comply with AML/CFT requirements are appropriately sanctioned. This is likely to require amendments of jurisdictions' legal frameworks to ensure that institutional measures (for example, the designation of a supervisory authority) and new requirements (for example, licensing and preventive measures) are established on a sound legal basis (see the discussion in "Virtual Assets and Anti–Money Laundering and Combating the Financing of Terrorism (AML/CFT)— Some Legal and Practical Considerations" in relation to legal foundations).

Licensing/Registration of VASPs

Like other professionals subject to AML/CFT measures (and unless VA activities are prohibited), VASPs require some form of official permission to operate. Jurisdictions have the option of submitting VASPs to either licensing or registration processes:[8]

- *Licensing* generally relies on certain criteria being met for the licensee to initiate and continue its activities.[9] A regulatory assessment is conducted ex-ante (that is, before the applicant is granted a license) and generally includes an assessment of whether the applicant meets the criteria for carrying out the regulated activities. These criteria would typically include a minimum level of resource requirements (such as financial capital, human resources, and physical location), corporate governance, internal controls and financial integrity requirements, and financial reporting and disclosure requirements. In the context of AML/CFT, it is particularly important for the licensing/registration process to screen out criminals from holding, or being the beneficial owner of, a significant or controlling interest or holding a management function in a VASP.
- *Registration* generally entails no or few prerequisites. In many instances, a regulatory assessment is conducted ex-post (that is, after an entity has been

[6]"12 Month Review of Revised FATF Standards - Virtual Assets and VASPs." https://www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html (.

[7]See: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html and http://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html. At the time of publication of this note, the current FATF guidance on the Risk-Based Approach to Virtual Asset Service Providers was being updated and the revised version expected to be published towards the end of 2021.

[8]The terms "licensing" and "registration" are not spelled out by the FATF, but in the traditional sense, they reflect different forms of official authorization, with the licensing regime (traditionally reserved for financial institutions) being a more stringent and more intrusive regulatory approach than a registration regime. More rarely, some countries have combined the two (that is, adopted a hybrid system in which entities, beyond being registered mandatorily, can obtain optional licenses that come with more stringent conditions and obligations but also with greater credibility backed by the regulator).

[9]On the legal complexities of licensing, and in particular the distinction between licensing criteria and procedure, see Bossu, W., and Chew, D., "But we are different! 12 Common Weaknesses in Banking Laws and What to Do about Them." IMF, WP/15/200, pp. 18–22.

registered), which will include the consideration of similar issues as noted previously.

The choice between a licensing and a registration regime depends on a jurisdiction's supervisory objectives and its approach to market entry. In addition to preserving financial integrity, such objectives include safeguarding the stability of the financial sector and providing consumer protection. Regardless of whether the jurisdiction adopts a licensing or a registration regime, it is imperative that it subjects VASPs to AML/CFT obligations and that the purpose of regulation and supervision (for example, AML/CFT only or AML/CFT and prudential) be made clear.

Given the virtual and borderless nature of VA activities, licensing or registration in at least one jurisdiction is key to ensuring that no VASP falls into a regulatory gap. Traditional financial institutions are authorized where they operate, but the internet-based and borderless nature of VA activities often makes it difficult to determine where VASP operations take place. To avoid potential regulatory gaps, the FATF established a minimum locus for licensing or registration, which varies depending on the type of VASP: (i) VASPs that are natural persons are, at a minimum, to be regulated based on their place of business;[10] (ii) VASPs that are legal persons should, at a minimum, be licensed or registered in the jurisdiction where they are "created," either through incorporation or any other mechanism used. Beyond the minimum standard, jurisdictions may go further by regulating VASPs that are offering services in the jurisdiction to their citizens or residents, even if the VASPs are located overseas. They may also extend their regime to include VASPs that are not created in their jurisdiction but conduct operations from their jurisdiction. As a result, it is likely that, in many instances, a single VASP operating in multiple jurisdictions will be subject to multiple licensing or registration regimes.

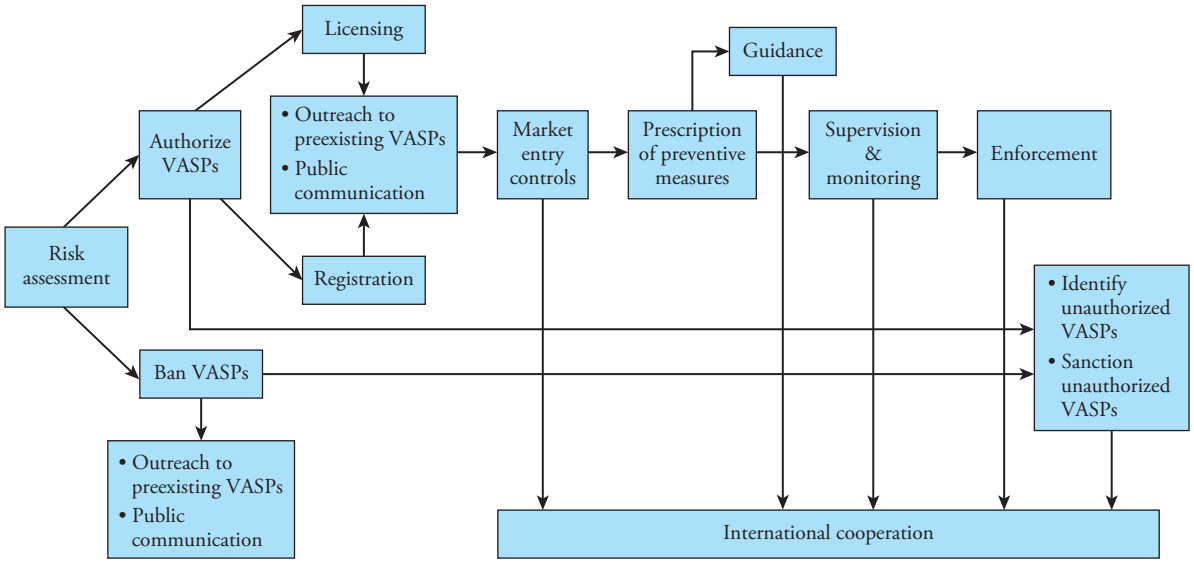
Jurisdictions need to designate one or more agencies for the authorization and subsequent supervision of VASPs. They may decide to leverage on existing regulatory and supervisory structures and designate one or more existing agencies to authorize and supervise VASPs, or create a new agency dedicated to the supervision of VASPs. Amendments to the existing legal framework may be necessary in both instances to ensure that there is an appropriate legal basis for licensing or registration, monitoring implementation of AML/CFT requirements, and sanctioning failure to comply with these requirements. Though self-regulatory bodies could play an important role, they may not be sufficient as they are not established by governments and often have an advocacy role that may conflict with supervisory duties. Unlike conventional financial institutions (for example, banks), where prudential or conduct supervisors often play the lead role in the licensing process, VASPs are often not subject to other requirements so AML/CFT supervisors will need to play a greater role in licensing or registration. All the supervisors involved should be prepared in terms of knowledge and resources before launching the framework. Where there is a large exisiting VASP population, careful planning is required to roll out the framework smoothly.

Jurisdictions should also be proactive in the enforcement of the regulatory framework. This notably requires outreach and engagement with VASPs to ensure that they understand their AML/CFT obligations. The approach should also include proactive identification of unauthorized VA-related activities by the relevant authorities. To this effect, all stakeholders, including the Financial Intelligence Unit (FIU) and law enforcement agencies, should work alongside the authority designated to supervise VASPs. A range of techniques and resources can assist in the identification of unauthorized activities.[11] Enforcement action against unauthorized operators should be wide-ranging to ensure credible deterrence. Enforcement actions typically include issuing warnings and alerts to the public about unauthorized firms and individuals; prohibiting and suspending individuals from carrying on unauthorized VA activities; deactivating the associated websites; imposing regulatory fines; and bringing (criminal) charges. Oftentimes, however, it may be challenging to take enforcement action, particularly when operators are based abroad, with no focal point (that is, purely online operations). In such cases, jurisdictions should conduct joint operations with relevant overseas

[10]This could be the primary location where the business is performed, where the business' books and records are kept, or where the natural person resides. These activities may be in one or more jurisdictions.

[11]For example, web crawling, feedback/whistleblowing received from the general public, suspicious transaction reports (STRs), information on past unsuccessful applications or regulatory history, financial intelligence provided by the FIU or law enforcement agencies, VASP advertisements in open-source information, and so on.

Figure 1. Actions Envisaged Under Policy Decisions on Whether to Authorize or Ban VASPs



Source: IMF staff.

authorities to take enforcement actions against unauthorized operators.

This proactive approach also applies to jurisdictions that choose to restrict activities in VAs. Banning VAs might not be a desirable choice for jurisdictions as they will miss the opportunity that VAs may offer and could possibly drive activities underground which would jeopardize financial integrity. Nevertheless, various factors can lead a jurisdiction to ban or limit the use of VAs on its territory, such as concern about misuse of VAs, limited capacity and resources to regulate and supervise VASPs and mitigate the risks related to VAs, or limited understanding of certain business models. Regardless of the scope of the ban, inactivity is not an option: specific measures are needed to mitigate domestic risk (for example, identification and enforcement action against illegal activities) and the broader international risk (for example, active contribution to international cooperation efforts). Unregulated VASPs, if not tackled, not only leave loopholes that can be exploited by criminals but also create opportunities for regulatory arbitrage jeopardizing the effectiveness of the global efforts to prevent them from being misused. Figure 1 illustrates what actions are envisaged under policy decisions to authorize or ban VASPs.

Preventive Framework

VASPs are the new "gatekeepers." To be effective, the prevention of ML and TF relies on those at the forefront of the interaction with the customers—the so-called "gatekeepers"—to identify and potentially thwart those that seek to misuse the financial system for criminal purposes. Given their interaction with customers, VASPs are required to implement the same types of measures as financial institutions and DNFBPs to bolster the prevention of ML/TF/PF.

To protect the integrity of the financial system, VASPs must implement a range of preventive measures. They include measures pertaining to customer due diligence (CDD); record-keeping; politically exposed persons (PEPs);[12] correspondent banking;[13]

[12]The FATF defines PEPs as individuals (including family members or close associates) who are or have been entrusted with prominent public functions by a 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) and distinguishes foreign from domestic PEPs. It also recognizes a third category of PEPs, namely persons (including family members or close associates) who are or have been entrusted with a prominent function by an international organization (members of senior management, that is, directors, deputy directors, and members of the board or equivalent functions). PEP checks are required to be carried out for both customers and beneficial owners.

[13]As set out in the FATF "Guidance for a Risk-Based Approach for Virtual Assets or VASPs," "To the extent that relationships in the

money or value transfer services; identifying, assessing, and mitigating the ML/TF risks that may arise in relation to new technologies; wire transfers; reliance on third parties; internal controls and foreign branches and subsidiaries; higher-risk jurisdictions; reporting of suspicious transactions; and tipping-off and confidentiality; and ensuring 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, TF, and PF.[14] Jurisdictions must ensure that secrecy laws do not inhibit VASPs from implementing AML/CFT obligations and certain preventive measures that deal with DNFBPs that engage in VASP activities. The main substance of and principles behind these obligations are the same for all three types of reporting entities (financial institutions, DNFBPs, and VASPs). The following paragraphs focus on some aspects where greater adaptation to the virtual space is needed. While the discussion that follows focuses on VASPs, it also applies to financial institutions when they are carrying out the activities of a VASP.

Setting Up Risk-Based Controls

Knowing and adapting to the risks is key. To be effective, the preventive framework should be commensurate to the risks. For VASPs, this means continuously modulating their approach on a risk basis, more specifically when:

- Establishing internal controls: This requires VASPs to identify and understand the ML/TF risks, as well as the risks of potential breaches, non-implementation, or evasion of the targeted financial sanctions related to PF ("PF risk" hereafter) prior to establishing how they intend to implement their AML/CFT obligations. To do so, VASPs need to carry out and document an enterprise-wide ML/TF/PF risk assessment that notably considers the following factors: customer, products and services, geographical regions, and delivery channels. In particular, the VASP should consider the specific types of virtual assets that the VASP offers and any unique features of VAs, such as whether they have anonymity-enhancing features, or whether they plan to offer services such as mixers or tumblers. These features may present higher risks (as discussed in "Virtual Assets and Anti–Money Laundering and Combating the Financing of Terrorism (AML/CFT)— Some Legal and Practical Considerations") by potentially obfuscating transactions or undermining a VASP's ability to undertake CDD and mitigate their ML/TF/PF risks. Once the risks are identified and understood, VASPs need to design and implement commensurate preventive controls to stop ML/TF/PF from occurring and detect it when it does. VASPs may use technological solutions to assist in performing enterprise-wide risk assessment as well as implementation of AML/CFT control measures.
- Establishing Risk-Based CDD Measures: Customer risk assessments must be carried out in all cases. The starting point involves collecting information to determine the purpose and intended nature of the customer relationship that assists in understanding the associated ML/TF/PF risks. Once the extent of ML/TF/PF risk a specific new customer poses has been established, VASPs need to determine the extent to which CDD measures should be carried out. This includes identifying and verifying the beneficial owner(s) for customers who are legal persons. Certain heightened risk factors (for example, customers who are PEPs or are from high-risk jurisdictions)[15] will require enhanced measures, while proven low risks may justify simplified measures. To ensure that CDD measures remain appropriate and to establish whether additional measures are required, VASPs will need to revisit customer risk assessments at regular intervals (the frequency depending on the level of risk associated with a customer) or based on the detection of a trigger event, such as a change in customer behavior/profile. The non-face-to-face environment in which VASPs typically operate requires specific changes to the way customer identification is usually performed.
- Monitoring the business relationship will be necessary in all cases to establish whether specific transactions fall outside the customer's normal pattern and are potentially suspicious. But the intensity of that

VASP sector currently have or may in the future have characteristics similar to cross-border correspondent banking relationships, countries should implement the preventive measures set out in Recommendation 13 to VASPs (and other obliged entities operating in the VA space) that develop such relationships."

[14]In some jurisdictions, lists of sanctioned Bitcoin addresses have been released.

[15]See, in particular, "FATF High Risk and Non-Cooperative Jurisdictions" https://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/more/more-on-high-risk-and-non-cooperative-jurisdictions.html?hf=10&b=0&s=desc(fatf_releasedate).

Box 1. Digital ID

The FATF published guidance on digital identification ("digital ID"), which clarifies how and the extent to which a digital ID is appropriate for use for customer due diligence purposes. The guidance highlights that financial institutions (including VASPs) can use "documents" as well as "information or data" when conducting customer identification and verification, and that there are no restrictions on the form (documentary/physical or digital) that identity evidence can take. The key element rests on ensuring that, in the digital context (as in the nondigital context), "reliable, independent source documents, data or information" are being used, which means potentially assessing these "new" forms of identification on a case by case basis to ensure that they meet this standard.

monitoring will vary depending on the customer's risk ranking.

Customer Identification

In an increasingly non-face-to-face environment, new methods of identification and verification of potential customers are emerging. Traditional means of carrying out CDD typically involve face-to-face engagement with the customer and the submission of physical identification documentation. These do not work well in a virtual environment. Jurisdictions should therefore consider the appropriateness of new methods (for example, electronic and biometric identification) as suitable alternatives. VASPs should seek to utilize all available information to carry out CDD. For example, as a starting point, unique user codes that may be linked to a customer can be used. Before relying on this information, however, controls should be in place to confirm the integrity of the information, and once the code has been linked to a customer, further steps should be taken to verify the identity of the customer.

VASPs must undertake CDD in a range of situations. A VASP may open and maintain customer accounts, and, as a result, these customers will usually fall into the category of a business relationship. CDD must be performed when a VASP enters into a business relationship with a customer and when it performs an occasional (one-off) transaction for non-customers above a certain threshold, which should be of US$/EUR 1,000 or less.[16] Recognizing the particular risks posed by virtual assets, this threshold is lower than the applicable threshold for financial institutions. The VASP will need to be in a position to demonstrate how it verifies that the transaction(s) are only conducted on an occasional (one-off) rather than a more consistent basis. VASPs must also conduct CDD where there is a suspicion of ML/TF or where they doubt the veracity or adequacy of previously obtained CDD information.

Certain information must be obtained for all customers, even those who carry out occasional transactions below US$/EUR 1,000.[17] The threshold for an occasional transaction may be a single operation or in several operations that appear to be linked. As such, VASPs will need to collect certain customer information for all transactions, even those below the threshold for an occasional transaction to effectively link transactions.[18] For example, in the scenario where there is a nonrecurring request from a customer to a VASP to convert VAs to cash that falls below US$/EUR 1,000, certain customer information (for example, name) will need to be obtained to ensure that there is a mechanism to track the customer's transactions and detect if the customer reaches (on a linked basis) the occasional transaction threshold, at which point full CDD measures must be applied.[19]

Targeted Financial Sanctions

Like other reporting entities, VASPs play a key role in ensuring that terrorists and proliferation financiers are barred from accessing the financial system. The framework for targeted financial sanctions for terrorism, TF, and PF applies in the context of VAs to the

[16]Competent authorities are free to set a lower threshold if deemed necessary.

[17]Interpretive Note to FATF Recommendation 15.

[18]While certain VASPs may determine that unique identifiers are effective for the purpose of linking transactions, this is not the case for implementing targeted financial sanctions, which require the screening of person or entity names.

[19]In the context of this activity, obtaining certain customer information is also required to implement targeted financial sanctions.

same extent as in the context of traditional assets. VASPs, like financial institutions (FIs) and DNFBPs, are required to implement measures to prevent funds or other assets being made available, directly or indirectly, to or for the benefit of, any person or entity on designated lists.[20] This means VASPs should ensure that all transactions are screened against designated lists to prevent such actors from gaining access to the financial system. This screening will involve controls to detect any positive matches, the capability to freeze the account and/or stop the transaction immediately, and the mechanisms to report these matches to the relevant authorities and file a suspicious transaction report (per the requirements of the national framework).

Total anonymity interferes with the effective implementation of targeted financial sanctions. While certain VAs and VASPs seek to provide greater privacy, this should not interfere with the implementation of targeted financial sanctions measures. Total anonymity is therefore not an option for VASPs. While there is a threshold for conducting CDD on occasional transactions, such a threshold is not applicable in the context of targeted financial sanctions screening. All transactions must be screened to ensure that funds or other assets are not made available, directly or indirectly, to or for the benefit of, any person or entity on designated lists. Consequently, the names of the originator and beneficiary of transactions must be obtained in all instances to carry out this screening effectively. Although full CDD measures are not necessarily required, certain additional information (for example, proof of identity documentation, information, or data) must also be obtained to verify the accuracy of the names that have been collected and subsequently checked against the various lists.

Record-Keeping

Information on customers and their transactions must remain available to competent authorities if and when necessary. Like other reporting entities, VASPs should maintain that information. For information on transaction, the obligation may be easier with the use of digital ledger technology (DLT), since the latter acts as an immutable ledger and, if properly maintained, holds the capabilities to record comprehensive information along with a trail to trace all transactions. However, reliance solely on the DLT is not sufficient. VASPs must "connect the dots" and link the transaction information available on the DLT to the relevant customer/beneficiary. The information available and level of accessibility will depend on the specific DLT being utilized. Therefore, before the use of DLT, or any technological solution, VASPs should ensure that they have a thorough understanding of the specific technology along with any limitations to ensure that compensatory controls are implemented, where necessary, so as to enable them to "connect the dots."

Wire Transfer Rules and the So-Called "Travel Rule"

Preventing and detecting ML/TF/PF requires VASPs to know who the originator and beneficiary of that transaction are. As a result, some information, such as the identity of both parties, must "travel" with the VA, similar to how it accompanies a wire transfer between banks—this is commonly called the "travel rule" but these rules apply in an amended manner to reflect the specific nature of VA transactions.[21] When transferring VAs, VASPs must therefore obtain, hold, and transmit required originator and beneficiary information. This requirement poses several challenges for VASPs, including implementing secure mechanisms for the transfer of information and ensuring that the required information accompanies the transfer in "real time." There are various technologies and tools available that could enable VASPs to comply with aspects of the travel rule requirements. At the moment, however, there are not sufficient technological solutions that enable VASPs to comply with all aspects of the travel rule in a holistic, instantaneous, and secure manner. Work is currently underway, and a few initiatives are being developed that could potentially assist VASPs in finding a solution.[22] Absent a global solution to implement the "travel rule" (akin to the SWIFT messaging system in

[20]Any person or entity designated (i) by, or under the authority of, the United Nations Security Council (UNSC) under Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267 (1999) and its successor resolutions; or (ii) pursuant to UNSC resolution 1373 (2001).

[21]Discussions are underway, including in the context of the public consultation held by the FATF on what these obligations entail in the context of the transfer of VAs and the potential data protection and privacy complications. The revised "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" (forthcoming) will provide further clarification.

[22]For example, the interVASP's IVMS-101 Messaging Standard (developed by a Joint Working Group established by industry bodies), has the potential to assist with meeting the travel rule requirements through operating as a universal common language between VASPs, who could then design their own technological solution to implement the standard or engage a third party to assist in the development of the required technological solution. https://intervasp.org/ (accessed 08/25/2020).

the banking sector), a key challenge will be to ensure the interoperability of different systems.

Monitoring and Reporting of Suspicious Transactions

Careful monitoring of the customer's behavior and transactions is key as it will enable the identification of potential suspicious activity. A robust system for the monitoring and detection of ML/TF activity should be implemented with a level of sophistication commensurate to the size and scale of the VASP's activities along with the level of exposure to ML/TF risk. The system should include VA ML/TF red flag indicators that are based on ML/TF typologies associated with VA activities (see Annex 2). VASPs should not overly rely on the identification of single indicators and remain cognizant that a typology will often involve multiple red flags that, in aggregate, may lead to a suspicion of potential ML/TF.

VASPs should then report suspicious transactions to the FIU. To bring suspicious activity to the attention of the FIU, VASPs and other reporting entities that engage in VA financial activities or operations or provide VA products or services need to ensure that there is a mechanism in place for the timely reporting of suspicions. In addition, jurisdictions will need to determine, for VASPs operating across multiple physical jurisdictions, which FIU in which jurisdiction should be the recipient(s) of these reports. The quality of information provided is crucial, as it is based on this information that an initial determination is made by the FIU as to whether further investigation is warranted. A suspicious transaction report (STR) should contain all relevant details relating to the suspicion raised, including information relating to the customer(s); the date(s) of the transaction(s); a rationale to support raising the suspicion; and all other relevant information. Unless this is already included in the reporting template,[23] FIUs should also determine whether there are additional forms of information that may be unique to VA activities that could assist in the assessment of suspicious activity, for instance, device identifiers, VA wallet addresses, and transaction hashes. Accordingly, jurisdictions should consider whether updates to existing reporting mechanisms or forms are required to facilitate VASPs and other reporting entities submitting information specific to VA activities.

New technologies may significantly enhance the detection of suspicious activity. Artificial intelligence (AI) and machine learning capabilities are increasingly used to facilitate and speed up the detection of potential suspicious activities. With AI's continually evolving algorithms and real-time decision-making abilities, such solutions may assist when dealing with large quantities of information and in identifying patterns or trends of suspicious behavior. However, FIUs and supervisors should stay on top of the evolution of these technologies and there remains a need for VASPs and supervisors to ensure that such solutions are challenged/assessed on an ongoing basis to ensure that they remain fit for purpose. For instance, AI solutions are only capable of recognizing known suspicious patterns and thus need to be enriched on an ongoing basis to keep up with the new patterns or schemes used by criminals. As such, caution should be exercised when using new technologies to assist in the detection of suspicious activity to prevent an overreliance on such technology. Further, VASPs must ensure that an adequate level of knowledge of any such tools is maintained in-house at both the commencement of use and on an ongoing basis thereafter. VASPs must identify and assess the ML/TF risks that may arise in the use of new or developing technologies.

Supervision/Monitoring of VASPs' Compliance with AML/CFT Requirements

Effective implementation of AML/CFT requirements can only be achieved when all stakeholders, including supervisors and VASPs, work closely with one another. Supervisors should work with other competent authorities and the private sector to understand the ML/TF/PF risks and help VASPs understand their own risks. Supervisors should clearly communicate their regulatory expectations and provide guidance and feedback to the VASP sector through different means, including ongoing dialogue with the sector and VASP-specific AML/CFT guidance. Where there are multiple supervisors for VASPs, it is also important that these bodies collaborate and share information to ensure a coordinated and consistent approach to supervising VASPs.

Like supervisors of other regulated entities, VASP supervisors should apply a risk-based approach to AML/CFT supervision. Before they can effectively do

[23]See "Virtual Assets and Anti–Money Laundering and Combating the Financing of Terrorism (AML/CFT)— Some Legal and Practical Considerations," page. [16].

so, they need to develop a thorough understanding of the ML, TF, and PF risks posed by the VASP sector compared to other sectors, as well as the risks within the VASP sector (if necessary, by ranking VASPs into sub-categories) at the VASP-entity level. Such assessments should be informed by the risks identified at the national level (and a developed understanding of VASPs' business models and operations).[24] Understanding of risks is a dynamic exercise and should be kept up-to-date. Supervisors can draw from several sources to inform their understanding of the risks. They may distribute supervisory returns to VASPs requesting information on their business model and associated AML/CFT systems and controls. In addition to information shared by the FIU and law enforcement agencies, AML/CFT supervisors can gain useful insights from data on interbank settlements related to VASPs and crypto asset blockchain explorers as well as public information, among others.

In assessing the risks at the entity level, supervisors should have regard to the inherent risks to which a specific VASP is exposed as well as the robustness of its AML/CFT controls. The assessment of inherent risks should notably consider four main groups of risk factors: customers, products and services, geographic regions, and delivery channels. These should include but are not limited to higher-risk factors in each group (for example, foreign PEPs) that must be met with enhanced CDD. Supervisors should seek to capture all major ML/TF/PF risks faced by VASPs, for example, risks associated with products with enhanced anonymous features, including internet protocol anonymizers or features that undermine the operators' ability to identify customers and beneficial owners (such as mixers and tumblers),[25] or links to multiple jurisdictions in terms of clientele or operations that would tend to mean higher risks by virtue of a wider spread of exposures and possibly fragmentation of the whole picture. When assessing the quality of a VASP's AML/CFT controls, regards should be given to its business model and whether the controls are commensurate with the level of risks in the VASP, for instance, whether robust controls are applied to remote customer identification/verification and authentication.

[24]See "Virtual Assets and Anti–Money Laundering and Combating the Financing of Terrorism (AML/CFT)— Some Legal and Practical Considerations," p. [14].

[25]These are commonly understood as services that may further obfuscate transactions or undermine the VASP's ability to implement CDD measures.

A good understanding of ML/TF/PF risks enables the determination of the most appropriate supervisory strategy. Guided by their understanding of ML/TF/PF risks, supervisors should target resources toward the higher-risk VASPs, which could involve enhanced offsite and onsite supervisory engagement strategies. An enhanced strategy could involve more frequent and in-depth inspections and closer offsite monitoring through desk-based reviews of materials on a regular and ad hoc basis. Supervisors should stay vigilant in seeking out emerging risks or issues across the sector and address them, including by conducting thematic inspections.

The modalities of supervisory inspections for VASPs might be different from those applicable to traditional FIs. In the context of FIs, onsite inspections essentially allow supervisors to test how well an entity's AML/CFT internal controls work in practice. Supervisors should expect to see an AML/CFT control framework that is adequately tailored to address the specific risks that the VASP faces. It should, at a minimum, include AML/CFT policies, procedures, and processes that are implemented to mitigate ML/TF/PF risk. Supervisors must challenge the adequacy of such frameworks and ensure that VASPs implement controls that are fit for purpose, including by the "live testing" of systems or technological solutions that are described in policies and procedures. Supervisors themselves should also adapt the modalities of inspection to a VASP in light of its specific characteristics, including, for instance, the type of its business (for example, exchange, custodian services, and so on) and corporate structure (for example, whether it is a new standalone entity or part of an existing financial group). For conventional financial institutions, inspections often involve onsite visits to the premises of the institution, while for VASPs this might not be necessary or effective. The greater involvement of technology in VASPs' operations and their internal controls means that most of these tests would have to be conducted depending on the technological solutions employed, possibly remotely rather than onsite. Where necessary, supervisors may consider engaging third-party experts to ensure there is adequate knowledge and expertise to challenge and assess business models, complex systems, and associated IT solutions.

Supervisors may be faced with new types of AML/CFT controls used by VASPs. While the AML/CFT requirements for VASPs are the same as those that apply to more traditional sectors, the means by which

a VASP meets such requirements may look different and include, for example, digital ID for customer onboarding or using smart contracts for transaction execution. VASPs may further rely on "off-the-shelf" or "custom-built" regulatory technology (RegTech) solutions, including blockchain analytic software to assist in meeting AML/CFT requirements. Supervisors will need to ensure that VASPs maintain adequate oversight and control of such solutions so that they are regularly tested, renewed, and updated. Supervisors should assess the appropriateness and adequacy of such oversight on a case-by-case basis and challenge VASPs to demonstrate how they are meeting AML/CFT requirements and managing ML/TF/PF risks. Where a VASP outsources large portions of its framework, supervisors should test that the VASP maintains adequate oversight of such arrangements and implements a robust program of assurance testing and compliance monitoring. Supervisors should ensure that they have the necessary resources, skills, and capabilities to fulfill these tasks. They may need to invest in training, personnel, or other resources to gain the required experiences, tools, and expertise.

Noncompliance with AML/CFT requirements should be met with dissuasive, proportionate, and effective sanctions. When warranted by the severity of violations, consideration should be given to suspension or revocation of the license or removal from the registration and sanctioning of directors and senior managers.[26] Supervisors would need a thorough understanding of the VASP's business model and its AML/CFT internal control systems to be able to identify the individuals who should be held accountable for a breach, which is more challenging in the VA context with fewer human interventions, such as in the context of smart contracts. As VASPs often operate across borders, supervisors should consider publicizing the results of their enforcement actions and alerting their foreign counterparts.

Regulatory and Supervisory Cooperation

The often cross-border and online nature of VA activities makes international cooperation key to the success of effective regulation and supervision of VASPs. In practice, specific VASPs may be subject to the AML/CFT framework of multiple jurisdictions, especially in the context of so-called global stablecoins, given their potential mass adoption across the globe. At the licensing or registration stage, regulators may wish to consult foreign counterparts who have authorized or rejected an application of the particular VASP to understand its regulatory history and activities overseas. Similarly, supervisors can benefit from their foreign counterparts' experiences with the particular VASP and its compliance record. Establishing AML/CFT supervisory colleges has proved useful for supervisors of traditional financial sectors and would be a powerful mechanism to facilitate information sharing and exchange of views among supervisors of VASPs to tackle the supervisory challenges associated with entities operating in multiple jurisdictions. More generally, sharing of knowledge and experiences on VASPs among jurisdictions would help enhance their capacities to understand and mitigate the ML/TF/PF risks in the sector.

Conclusion

The new FATF standards for VAs constitute major progress. The 2018 and 2019 changes to the standards provide much needed clarity on what regulation and supervision of VASPs should look like. This is key in ensuring greater consistency in jurisdictions' approaches to mitigating the financial integrity risks of VAs and limiting regulatory arbitrage. By subjecting VASPs to measures similar to those already applicable to FIs and DNFBPs, FATF has ensured that the new actors in the virtual space are treated fairly and that similar risks are addressed equally. It has also increased the VASPs' chances of interaction with the traditional financial sector, including the banking sector—several VASPs have indeed indicated that the benefits of implementation of sound AML/CFT systems outweigh the costs, notably because it has reassured banks that the ML/TF/PF risks were sufficiently mitigated to enable them to engage in banking activities.

But implementation is challenging. As noted previously, while both the public and private sectors have made progress in the implementation of the standards for VAs, challenges remain, and, overall, implementation of the new standards is uneven.[27] In addition,

[26]See the FATF Guidance on "Effective Supervision and Enforcement By AML/CFT Supervisors of the Financial Sector and Law Enforcement" for more detailed guidance on enforcement.

[27]"12 Month Review of Revised FATF Standards—Virtual Assets and VASPs." https://www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html.

with the emergence of so-called global stablecoins, AML/CFT supervisors are likely to face increased challenges (for example, with a greater number of VASPs to supervise, greater business volume among existing VASPs, or greater market scale, hence the greater relative importance of the VASP sector). While encouraging innovation associated with VASPs, jurisdictions should make sure that they are ready to mitigate the financial integrity risks by ensuring that VASPs are subject to appropriate AML/CFT measures and that supervisors have the know-how, powers, and resources to monitor compliance effectively.

Protecting the financial system from the criminal misuse of VA requires continued focus and enhanced efforts. Going forward, jurisdictions and VASPs will need to step up their efforts and, for the most part, put in place the necessary measures and ensure their effective implementation to protect the financial system from ML/TF/PF activities and prevent regulatory arbitrage. The international AML/CFT community will also need to remain engaged, notably by continuing to monitor the financial integrity risks related to VAs with a view to ensuring that the standards remain appropriate. Sustained efforts are needed to assist jurisdictions in their implementation of the standards and address issues that may arise from the uneven implementation of and multiplicity of regulatory frameworks. In this respect, the FATF has committed to issue more guidance (for example, on so-called stablecoin, anonymous peer-to-peer transactions, the "travel rule," and red flags for potential ML/TF); promote the understanding of ML/TF/PF risks specific to VAs; engage with the private sector; work to enhance international cooperation among VASP supervisors; and to take stock periodically of the implementation of the standards on VA and VASP across the globe. Nonetheless, further guidance would be useful, for instance on the inspection of VASPs. IMF staff is committed to assist its members as appropriate in all its relevant workstreams, including through capacity development activities, with a view to strengthen financial integrity in the VA space.

Annex 1. FATF Standards Related to VAs and VASPs

Although the entire Financial Action Task Force (FATF) standards apply in the context of virtual asset (VA) activities, some specific provisions were introduced in 2018 and 2019 to address explicitly some VA- and virtual asset service provider (VASP)-related aspects:

Recommendation 15 "New Technologies," second paragraph:

"To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for [anti–money laundering/combating the financing of terrorism] 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."

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 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 [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 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 Rec-

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

ommendation 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 information[2] on virtual asset transfers, submit[3] 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 37–40. 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.

Glossary

Virtual Asset: 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 Providers: 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) transfer of virtual assets;[4] (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 virtual assets.

[2]As defined in INR [Interpretive Note to Recommendation] 16, paragraph 6, or the equivalent information in a VA context.

[3]The information can be submitted either directly or indirectly. It is not necessary for this information to be attached directly to VA transfers.

[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.

Annex 2. ML/TF Red Flag Indicators

In an effort to guide virtual asset service providers (VASPs) in the detection of potential illegal activities, both the Financial Action Task Force (FATF) and countries have established lists of examples of red flag indicators that may be included in a transaction monitoring (system.

The FATF recently published a list of virtual assets—red flag indicators. Countries should ensure that these flags are incorporated (where applicable) into transaction monitoring systems. More crucially, VASPs should use the six categories highlighted in the report as a framework from which to identify additional red flags tailored to their activities and associated ML/TF risk, as follows:

- Transactions
- Transaction Patterns
- Anonymity
- Senders or Recipients
- Source of Funds or Wealth
- Geographical Risks

The US Financial Crimes Enforcement Network[1] highlighted the following examples:

- A customer receives a series of deposits from disparate sources that, in aggregate, amount to nearly identical aggregate funds transfers to a known virtual currency exchange platform within a short period of time.
- A customer's transactions are initiated from non-trusted IP addresses, IP addresses from sanctioned countries, or IP addresses previously flagged as suspicious.
- A customer provides identification or account credentials (for example, non-standard password, IP address, or flash cookies) shared by another account.
- A common wallet address is shared between customers.
- A customer initiates multiple rapid trades between multiple virtual currencies with no related purpose, which may be indicative of attempts to break the chain of custody on the respective blockchains or further obfuscate the transaction.

[1]The Financial Crimes Enforcement Network, "Advisory on Illicit Activity Involving Convertible Virtual Currency" May 9, 2019.