Royal United Services Institute
for Defence and Security Studies

Guidance Paper 2021

Counterproliferation Financing for Virtual Asset Service Providers

Kayla Izenman

Counterproliferation Financing for Virtual Asset Service Providers

Kayla Izenman

RUSI Guidance Paper, September 2021

Royal United Services Institute
for Defence and Security Studies

190 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 190 years.

Disclaimer

This is a guidance paper for virtual asset service providers (VASPs) looking to build or further develop a counterproliferation financing (CPF) function within their organisation. The guidance aims to provide a framework for VASPs to apply and adapt their own financial crime compliance practices while remaining in line with domestic regulatory requirements. The guidance paper does not constitute legal or regulatory advice and should always be read in conjunction with relevant national legislation and international standards and guidelines, and independent legal advice should always be sought on sanctions, anti-financial crime and CPF implementation.

During the time of writing, Kayla Izenman was a Research Fellow in RUSI's Centre for Financial Crime and Security Studies. This paper represents her personal view during that time and does not represent the views of, nor relate to, the work she does now or her current employer.

The views expressed in this publication are those of the author, and do not reflect the views of RUSI or any other institution.

Published in 2021 by the Royal United Services Institute for Defence and Security Studies.

RUSI Guidance Paper, September 2021. ISSN 2397-0286 (Online).

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org
RUSI is a registered charity (No. 210639)

Contents

Acknowledgements

This study was conducted with generous support from the John D and Catherine T MacArthur Foundation. Thanks go to David Carlisle and Malcolm Wright for their helpful comments on an earlier version of this document. Thanks are also due to all those who have generously offered their time to be interviewed for RUSI's virtual asset research since 2017, as well as the RUSI publications team for their work on editing the guidance.

Acronyms

AML – anti-money laundering

CDD – customer due diligence

CTF – counterterrorist financing

CPF – counterproliferation financing

EDD – enhanced due diligence

FATF – Financial Action Task Force

KYC – know your customer

ML – money laundering

PF – proliferation financing

TF – terrorist financing

VA – virtual asset

VASP – virtual asset service provider

I. Scope and Objectives

PROLIFERATION FINANCING (PF) of WMDs is defined by the Financial Action Task Force (FATF) as 'the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons'.[1] This is the FATF's working definition, but it is worth noting that there is no internationally accepted definition of PF, and some have advocated for a broader understanding that might include, for example, revenue-generating activities.[2]

WMD proliferators, such as North Korea and Iran, continue to evade targeted financial sanctions. Virtual assets[3] (VAs) have increasingly become a vehicle through which proliferation-related funds are raised and moved. However, sanctioned WMD proliferators' high-level knowledge of VA laundering and fundraising has not yet been met with the requisite compliance, regulation and law enforcement action. The VA space has grown and improved in terms of compliance practices in the last few years, but some criminal actors remain ahead of the curve.

Sanctions targeting North Korea's nuclear weapons programme have been in place at the UN level since 2006, and have steadily expanded to include targeted financial sanctions against designated individuals and entities, activity-based sanctions restricting North Korea's ability to access the international financial system, and sectoral sanctions targeting specific sectors or exports from North Korea. The UN also maintains sanctions against certain Iranian individuals and entities, and restricts activities related to ballistic missile development.[4]

Since at least 2014, North Korea has shown increasing cybercrime expertise and interest, more recently expanding into VAs.[5] Throughout 2020 and 2021, the US Department of Justice indicted

1. Financial Action Task Force (FATF), 'Combating Proliferation Financing: A Status Report on Policy Development and Consultation', FATF Report, February 2010, p. 5.
2. For further discussion on the definition of proliferation financing (PF), see Anagha Joshi, Emil Dall and Darya Dolzikova, 'Guide to Conducting a National Proliferation Financing Risk Assessment', RUSI, May 2019, p. 5.
3. In this guidance paper, 'virtual assets' refer to digital payment tokens such as Bitcoin. For the full definition, please see the 'Terminology' section.
4. For up-to-date information on UN sanctions requirements related to proliferation, see UN, 'Subsidiary Organs of the United Nations Security Council', 2021. Unilateral sanctions, such as those imposed by the US, the EU or the UK, might impose additional requirements to those of UN sanctions.
5. One of the earliest instances of North Korean cybercrime activity was the infamous Sony Pictures hack, attributed by the FBI in December 2014. See FBI, 'Update on Sony Investigation',

a series of individuals for laundering VAs on behalf of North Korea.[6] Yet, while most North Korean VA activity involves large-scale hacks, such as the $49 million 2019 Upbit hack[7] or the $275 million stolen from KuCoin in 2020,[8] the regime has also shown interest in ransomware attacks and VA mining.[9] Overall, North Korea is highly advanced in the cybercrime realm and seems increasingly interested in applying these skills to cryptocurrency activities. Similarly, although not the core focus of this guidance paper, Iran has reportedly begun to use VA mining to evade sanctions and export oil, with a huge share of global VA mining taking place in the country.[10] With global compliance and regulation lacking in many jurisdictions, virtual asset service providers (VASPs) can present an easy target for these actors.

This guidance paper aims to advise VASPs on best-practice compliance when dealing with PF risk, and directs compliance officers towards relevant publications that may assist in their work (see Annex II). The paper will be particularly helpful to those VASPs who have not previously thought about PF or the implementation of targeted financial sanctions related to proliferation as a distinct financial crime or sanctions risk.

---

19 December 2014, <https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation>, accessed 24 August 2021.

6. US Department of Justice, 'Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe', 17 February 2021; US Department of Justice, 'United States Files Complaint to Forfeit 280 Cryptocurrency Accounts Tied to Hacks of Two Exchanges by North Korean Actors', 27 August 2020; US Department of Justice, 'Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency From Exchange Hack', 2 March 2020, <https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack>, accessed 24 August 2021.
7. For details on the Upbit hack, see Marie Huillet, 'Upbit Hack: Stolen ETH Worth Millions on the Move to Unknown Wallets', *Coin Telegraph*, 3 December 2019, <https://cointelegraph.com/news/upbit-hack-stolen-eth-worth-millions-on-the-move-to-unknown-wallets>, accessed 25 August 2021. The 2020 US Department of Justice complaint against Tian Yinyin refers to the Upbit hack as the 'November 2019 Intrusion and Theft' of 'Exchange 3'. US Department of Justice, 'Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency From Exchange Hack'.
8. For details on the KuCoin hack, see Chainalysis, 'The KuCoin Hack: What We Know So Far and How the Hackers are Using DeFi Protocols to Launder Stolen Funds', 2 October 2020, <https://blog.chainalysis.com/reports/kucoin-hack-2020-defi-uniswap>, accessed 25 August 2021. The 2021 UN Panel of Experts Final Report refers to an ongoing investigation into a 'hack against a cryptocurrency exchange that occurred in September 2020' resulting in 'approximately $281 million worth of cryptocurrencies stolen from the exchange'. 1718 Sanctions Committee (DPRK), 'Final Report of the Panel of Experts Submitted Pursuant to Resolution 2515 (2020)', 4 March 2021.
9. Yosuke Onchi, 'North Korea Ramps up Ransomware Attacks in Hunt for Cash', *Nikkei Asia*, 18 February 2021.
10. Tom Robinson, 'How Iran Uses Bitcoin Mining to Evade Sanctions and "Export" Millions of Barrels of Oil', Elliptic, 21 May 2021.

While this guidance uses proliferation case studies, mostly focusing on North Korea, much of it draws from typologies, red flags and best practice that can be found in other types of VA crime, especially when illicit activities are conducted by large criminal organisations that might have comparable expertise and funding to a sanctioned country.

The guidance follows the general structure of the compliance cycle, beginning with pre-requirements before client interaction, then moving to the onboarding process, followed by ongoing monitoring throughout the client relationship. After going through the cycle, the guide touches on high-risk indicators and red flags that could lead to enhanced due diligence or exiting of the client and concludes with reporting requirements following any flagged suspicious activity.

FATF Recommendations for Virtual Assets and Virtual Asset Service Providers

Understanding and implementing the FATF Recommendations for VASPs is key to best-practice compliance, and this guidance aims to match and support the FATF Recommendations.

While the FATF has acknowledged the risks associated with VAs since 2014,[11] the first VA-related adoption of changes to its Recommendations was in October 2018, clarifying that the Recommendations apply to financial activities involving VAs. In June 2019, the FATF adopted an Interpretive Note for Recommendation 15,[12] which further clarified how the FATF Recommendations apply to VAs and VASPs. This included guidance on supervision, monitoring, licensing and registration, customer due diligence (CDD), suspicious transaction reporting, sanctions screening measures and more.

The FATF also adopted the Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers in June 2019,[13] which aims to assist national authorities in developing appropriate regulatory regimes for VAs and VASPs, and also to advise private sectors on how to comply with these requirements.

There have been two reviews of the FATF Guidance since its publication, in July 2020 and July 2021.[14] The Guidance is also updated regularly to improve recommendations and stay current

11. FATF, 'Virtual Currencies: Key Definitions and Potential AML/CFT Risks', June 2014, <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>, accessed 25 August 2021.
12. FATF, 'Public Statement on Virtual Assets and Related Providers', 21 June 2019, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-statement-virtual-assets.html>, accessed 24 August 2021.
13. FATF, 'Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers', June 2019, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html>, accessed 24 August 2021.
14. FATF, '12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers', July 2020, <https://www.fatf-gafi.org/publications/fatfrecommendations/

with the pace of innovation in the VA industry, and to that end, the FATF engages in public consultations on the Guidance.[15]

International Requirements

This guidance paper aims to present a set of standards in line with the most stringent international recommendations and regulations on VA compliance. It should be noted, however, that it does not follow any specific national regulation of cryptocurrencies. Please ensure full understanding of the regulations for the relevant jurisdictions for the VASP before attempting to apply any of the advice found in this paper. In addition to this, and/or if regulation is not present in the relevant jurisdiction(s), ensure full understanding of the FATF Recommendations. See Annex I for more details.

documents/12-month-review-virtual-assets-vasps.html>, accessed 24 August 2021; FATF, 'Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers', July 2021, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html>, accessed 24 August 2021.

15. FATF, 'Public Consultation on FATF Draft Guidance on a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers', March 2021, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-consultation-guidance-vasp.html>, accessed 24 August 2021.

II. Terminology

THIS GUIDANCE PAPER uses the vocabulary employed by the FATF. Therefore, the terms 'virtual asset' (VA) and 'virtual asset service provider' (VASP) are used throughout.

Please note, although the term 'VASP' is used, the scope of this term is narrower than that of the FATF definition. While the FATF definition includes any business involved in VA-to-fiat exchange, VA-to-VA exchange, or the transfer, safekeeping, or administration of VAs, and any business providing financial services relating to VAs,[16] this guidance paper defines a VASP as a **centralised virtual asset exchange** offering VA-to-fiat or VA-to-VA services.

Similarly, the term VA is applicable only to **payment tokens**, such as Bitcoin, and does not refer to stablecoins or central bank digital currencies. In this paper, VA has equivalency to the terms 'cryptocurrency', 'virtual currency' or 'crypto-asset'.

VA 'wallets' come in a variety of forms, and this paper does not discriminate between hot (online) wallets and cold (offline) wallets. Wallets keep a user's private keys secure and accessible, and are offered by many providers, including centralised exchanges.

Methodology

This guidance was produced as part of RUSI's ongoing CPF project. The RUSI team has analysed PF activity since 2015,[17] including continuing research on the role VAs and other new payment systems play in sanctions evasion, largely focusing on North Korea.[18] This guidance is based on the RUSI team's expertise in this field, in-depth research and informal conversations over the past three years with stakeholders in relevant industries, including VASPs, regulators, law enforcement, traditional banks, challenger banks and academia.

16. FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations', updated June 2021, p. 130.
17. For more RUSI PF publications, see RUSI, 'Proliferation Financing', <https://rusi.org/explore-our-research/topics/proliferation-financing>, accessed 24 August 2021.
18. For more detailed information on North Korean VA activity, see David Carlisle and Kayla Izenman, 'Closing the Crypto Gap: Guidance for Countering North Korean Cryptocurrency Activity in Southeast Asia', *RUSI Occasional Papers* (April 2019).

III. Pre-Requirements

THIS SECTION FOCUSES on all aspects of the compliance system required to be in place prior to onboarding any customers. This includes an effective and knowledgeable compliance team, initial risk assessments, a thorough understanding of all relevant national and international requirements, proper cybersecurity training and protocols, and a bespoke policy regarding coin listing decisions.

Compliance Team

In order to properly implement any of the following guidelines, VASPs must first ensure they have the proper governance structure and compliance team in place. A VASP's organisational structure should ensure that the compliance function has the resources, authority, information and independence necessary to assess and manage anti-financial crime risks.

A comprehensive governance structure considers all tiers of the business. Senior management should hold ultimate responsibility for the oversight and effectiveness of the anti-financial crime programme.

An effective programme also requires a compliance officer, usually named the Chief Compliance Officer, who is ultimately responsible for designing and implementing the compliance programme, as well as ensuring all compliance with regulatory and legal obligations. In larger companies, there may be an additional designated Sanctions Compliance Officer to ensure oversight and compliance with sanctions-specific requirements.

Mid-level and junior staff at all levels of the organisation should also be briefed on transaction red flags, screening and reporting requirements, investigation methods, and other relevant compliance procedures that could manifest in other areas of the VASP's business operations.

Some regulated jurisdictions require specific roles within the compliance team. Management must ensure that these are taken into consideration when building a compliance team. All staff in the compliance team should be regularly trained on any new VA trends, VA-specific compliance tools, and all relevant local, national and international regulation.

Risk Assessment

VASPs should regularly undertake an internal risk assessment to identify clients, sectors or transaction types which may be more exposed to money-laundering (ML)/terrorist-financing (TF)/PF activity – and to design and implement controls to mitigate those specific risks. Risk assessments are regularly undertaken on similar topics by financial institutions, and VASPs should likewise adopt this approach.

Risk assessments should be recorded in writing and be available for inspection by regulators. Risk assessments consist of three elements: threats; vulnerabilities; and consequences.

In the PF space, the FATF considers that 'threat' refers to any person or entity that has previously evaded, breached or exploited PF sanctions, or has the potential to do so in the future. 'Vulnerabilities' are anything that can be exploited by the threat, for example, gaps in regulation or cybersecurity weaknesses. This includes geographical and sector-specific vulnerabilities. 'Consequences' refer to the outcome wherein funds or assets become available to designated threat actors, not only in terms of financing WMDs, but also regarding the ultimate impact on the VASP's business operations and reputation.[19]

The line between threats and vulnerabilities can be blurred, but it is important to understand the interaction between the two, alongside any mitigating factors. When looking at threats and vulnerabilities, take into account at least the following considerations:

- Known threat actors.
- Known financing crime typologies.
- Size and complexity of the VASP.
- Products and services offered.
- Method of product and service delivery.
- Types of customers.
- Physical location of customers.
- Physical location of the VASP and relevant regulations.
- Related institutions.

The outcome of a risk assessment should indicate to a VASP in which areas its inherent risks are particularly high. Inherent risk is generally defined as the amount of risk that exists in the absence of controls, information that will become clearer following a comprehensive risk assessment. These controls should be considered mitigating factors in the risk assessment.

The potential consequences of PF are more severe than those of ML or TF. VASPs should assess physical, social, environmental, economic and structural impacts and harms.

For further information on conducting risk assessments for VASPs, see Annex I.

Cybersecurity

In addition to compliance procedures, given the extent to which cyber attacks are deployed to fund proliferation, it is essential to have a focus on cybersecurity. This includes both education of VASP staff of all levels as well as investment in cybersecurity professionals to install appropriate safeguards for the VASP.

19. For further information on the definitions of these three elements, see FATF, 'Guidance on Proliferation Financing Risk Assessment and Mitigation', June 2021, p. 9.

Educating staff on cybersecurity protocols is essential to protect against hackers working on behalf of proliferators. North Korea especially has been known to be involved in complicated phishing schemes in order to infiltrate VASPs, such as its attack on DragonEx in 2019.

Case Study 1: DragonEx (2019)

In March 2019, North Korea executed an elaborate phishing scheme leading to an employee of the VASP DragonEx unknowingly installing malicious software in a computer containing private keys of the VASP's wallet, allowing North Korea to steal millions of dollars in virtual assets. Researchers found that the Lazarus Group, a North Korean cybercriminal group, was responsible for the attack, leading to a loss of over $7 million.

Lazarus registered two internet domains, faked VA trading software and embedded it with malicious code, and hid the deception within an automated VA trading platform which operated normally for six months. Attackers then sent the software to staff at a variety of VASPs, under the guise of product promotion. Customer service staff at DragonEx opened an installation package of the malicious software, through which the hackers were able to obtain the private key for the VASP's wallet and carry out the theft.

Sources: Lylian Teng, 'Alert! Lazarus Hacker Group Continues Targeting Crypto Using Faked Trading Software', 8BTC, 1 April 2019, <https://news.8btc.com/alert-lazarus-hacker-group-continues-targeting-crypto-using-faked-trading-software>, accessed 24 August 2021; Chainalysis, 'As Exchanges Beef Up Security Measures, Hackers Get More Sophisticated', 21 January 2020, <https://blog.chainalysis.com/reports/cryptocurrency-exchange-hacks-2019>, accessed 25 August 2021.

Education is key, as is physically securing the VASP from these types of attacks. Staff should be required to undergo regular cybersecurity training sessions and know what to expect and how to identify potentially suspicious emails, attachments, links and programmes. *All* staff should be required to undergo these sessions, not only those involved in the compliance programme. VASPs should also specifically invest in an appropriate IT and cybersecurity infrastructure to ensure attackers are unable to infiltrate the system from the outside.[20]

Asset Listing Requirements

Given criminal actors' increasing interest in privacy coins, which potentially allow them to move VAs undetected, it is key to consider the blockchain tracing abilities for any asset being listed on a VASP's platform. There are a variety of options that may help mitigate risks posed by privacy coins. One option is simply to exclusively offer assets with transparent blockchains (in other

20. For more information on recommended cybersecurity safeguards, see Cloud Security Alliance, 'Crypto-Asset Exchange Security Guidelines', 13 April 2021, <https://cloudsecurityalliance.org/artifacts/csa-crypto-asset-exchange-security-guidelines-abstract/>, accessed 22 August 2021.

words, not accepting any privacy coins at all). If this is not an appropriate solution, and listing privacy coins is an accepted risk and part of a VASP's commercial strategy, the following risk mitigations should be considered:

- Listing only a select choice of privacy coins which have at least some measure of transparency (for example, Zcash) and for which blockchain tracing analysis is available.
- Allowing use of privacy coins *only* in cases of VA-to-VA transactions (in other words, allowing privacy coins to be traded for other VAs, but not fiat currencies) in an effort to hinder fiat cash-out.
- Only allowing customers to trade in privacy coins where they undergo enhanced due diligence (EDD) and where trading in privacy coins is subject to strict limits and thresholds.

IV. Sanctions and PEP Screening

SANCTIONS APPLY TO all clients and transactions, no matter the amount. VASPs should adhere fully to international and relevant national sanctions lists to avoid holding accounts for designated actors, or anyone owned, controlled, acting on behalf of or at the direction of designated actors. Sanctions screening should be conducted at first identity verification and regularly throughout the client relationship,[21] for any incoming and outgoing transactions, or when there are additions to the sanctions lists.

The US Office of Foreign Assets Control (OFAC) has also previously included VA addresses on its sanctions list, which should be flagged in addition to any listed names.[22] OFAC has also sanctioned many individuals and groups for VA-based sanctions evasion activity. It is recommended that the US sanctions lists are considered in addition to any international lists. OFAC has specifically included VA addresses belonging to actors laundering on behalf of North Korea, showing the importance of these lists in addressing proliferation finance risk.

Case Study 2: Tian Yinyin and Li Jiadong (2020)

In March 2020, OFAC sanctioned Tian Yinyin and Li Jiadong, two Chinese nationals laundering VAs on behalf of North Korea. These actors were sanctioned under the US CYBER2 and DPRK3 programmes, and noted as linked to the North Korean hacking group, the Lazarus Group.

The OFAC listing for each individual includes not only their personal information, but also any known associated Bitcoin addresses. Tian, for example, has eight Bitcoin addresses listed. The listings also include known aliases, in this case the perpetrators' online IDs.

Source: For more information on the OFAC listings, see US Department of the Treasury, 'Treasury Sanctions Invididuals Laundering Cryptocurrency for Lazarus Group', 2 March 2020, <https://home.treasury.gov/news/press-releases/sm924>, accessed 24 August 2021; OFAC, <https://sanctionssearch.ofac.treas.gov/Details.aspx?id=28263>, accessed 24 August 2021.

21. For example, when client details (directors, ownership, identifying details) change.
22. This practice began in 2018, when OFAC listed the VA addresses of Iran-affiliated cyber actors. See US Department of the Treasury, 'Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses', press release, 28 November 2018, <https://home.treasury.gov/news/press-releases/sm556>, accessed 24 August 2021.

In addition to sanctions lists, any actors or groups mentioned in the UN Panel of Experts' reports should be included in sanctions screening. For more information on these reports, see Annex I.

VASPs should also consider media screening and consultation of typology reports by NGOs and the private sector, including blockchain analytics companies and cybersecurity firms. These actors regularly publish findings both on red flags of North Korean use of VAs as well as North Korea-affiliated individuals and organisations. Similarly, VASPs should both screen clients and continue monitoring to check if they are (or are interacting with) a politically exposed person (PEP).[23] If so, EDD should be undertaken. For further guidance on EDD, see below.

23. The FATF defines a politically exposed person (PEP) as 'an individual who is or has been entrusted with a prominent function', and who may be 'in positions that can be abused for the purpose of … laundering [illicit funds]'. See FATF, 'FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22)', June 2013, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf>, accessed 22 August 2021.

V. Onboarding

ONBOARDING IS THE next step in the compliance cycle. VASPs often have concerns about the level of information required from customers on first contact. While businesses may operate differently, and jurisdictions will have varying requirements, there are some common principles and best-practice activities that will ensure the highest possible chance of detecting suspicious activity.

Know Your Customer Processes

Know your customer (KYC) processes are standard in banks and should be equally standard in VASPs. Unfortunately, a 2020 report indicated that 56% of global VASPs have weak or porous KYC processes.[24] Simple initial steps can be taken to ensure a VASP does not fall into this group.

Many VASPs allow account creation with no identity verification but require additional information to send or receive funds. Some VASPs even require verification before account creation, while others only require KYC when involving fiat currency.

Best practice dictates that KYC should take place *before* funds are deposited or accepted by the customer, whether this means at the time of account creation or immediately before the first transaction is initiated.

The first consideration is customer identification and verification of that identity. While regulatory authorities might require additional specific information, at a minimum the following pieces of information should be collected from individuals:

- Name, date of birth and nationality (verified using official government identification process).
- Address verified using a proof of address document, such as a bank statement, utility bill, government-issued tax letter, home insurance document, or certificate of residence, or via digital means that provide reasonable surety on the customer's physical location.

In addition, at a minimum the following pieces of information should be collected from legal entities:

- Name, registration, address and status (verified by company number or relevant government registration documents and registries).

---

24. CipherTrace, 'CipherTrace 2020 Geographic Risk Report: VASP KYC by Jurisdiction', October 2020, p. 4, <https://ciphertrace.com/2020-geo-risk-report-on-vasp-kyc/>, accessed 24 August 2021.

- Identifying information of key management personnel, including authorised traders on the customer's account.
- Ownership structure.

KYC (and continual CDD) should be conducted not only on customers themselves, but also any beneficial owners, as well as any persons acting on behalf of the customer.

VASPs should also ensure that their processes for verifying information are comprehensive. This includes requesting the above official documents and ensuring their legitimacy, as well as considering further KYC mechanisms, either during onboarding or at the time of a suspicious transaction. These further requirements may include:

- Selfies taken within the app itself, including a 'liveness' test, to prove that the face uploaded is from a live person present at the point of capture.
- Video calls.

Identity verifications and liveness tests are key to effective compliance, especially when it comes to the tactics employed by actors involved in proliferation finance. In 2020, launderers moving funds on behalf of North Korea could not fulfill the video call compliance requirements at one VASP, which ideally would have prevented the funds from being laundered through the platform.

Case Study 3: 'VCE3' (2020)

In the same case as described in Case Study 2, in addition to the OFAC sanctions, the US Department of Justice charged Tian Yinyin and Li Jiadong with laundering over $100 million in various cryptocurrencies on behalf of North Korea. The coins were gained from North Korean VASP hacks, and Tian and Li attempted to move the funds through multiple VASPs, with largely successful results.

In order to provide sufficient documentation to VASPs during the onboarding process, Tian and Li edited photos of individuals using stolen personal identifiable information. One VASP (referred to as VCE3) was unsatisfied with the image provided and requested a video call with the account holder, which was denied. Despite this, VCE3 accepted transactions from Tian and Li, receiving almost $2 million of the stolen funds into the criminal actors' account. This indicates that had a live video call been a compliance requirement of all involved VASPs, the funds may not have been laundered through the platforms at all.

Source: US Department of Justice, 'Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency From Exchange Hack', 2 March 2020, <https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack>, accessed 24 August 2021.

Nature and Purpose of Relationship

Equally as important as the identification of the customer is the nature and purpose of the customer relationship. The only way to effectively understand what suspicious activity looks like for a specific customer is to understand what regular activity looks like, or is expected to look like, for that customer. In order to fully understand the nature and purpose of the relationship during onboarding, the following estimates, at a minimum, should be requested from the customer:

- Expected frequency of transactions.[25]
- Expected size of transactions.
- Expected volume of transactions.

Source and Destination of Funds

It is essential, as a VASP, to understand both the source and destination of any funds being moved through the platform. In particular, where EDD is required, VASPs should gather information about a customer's source of funds and verify legitimacy before conducting any business on behalf of the customer. For further guidance on EDD, refer to the dedicated section later in the paper.

Similarly, when a customer is receiving funds or engaged in transactions, the VASP should attempt to gather relevant information about the other party.[26] Blockchain analytics tools can provide enhanced insight into the ultimate source and destination of funds, and are a recommended step in achieving this.

25. Here, 'transaction' refers to deposits, withdrawals and trades.
26. The full possibility of this is under discussion, in line with the FATF's Recommendation 16. For now, exchanges should request the information they are able to gather from customers. See FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations', p. 17.

VI. Ongoing Monitoring and Customer Due Diligence

FOLLOWING ONBOARDING, THE next stage is to ensure continued and effective CDD on existing customers. This means transaction monitoring in an effort to identify any unusual activity, such as deviation from expected or anticipated transaction activity, and understanding the reasoning and purpose behind any variation that is found on the platform. Unusual or suspicious activity that is unable to be explained by the customer may indicate ML/TF/PF connections. There should be constant scrutiny of customer activity throughout the course of the relationship to ensure that the activity is consistent with the KYC process conducted during onboarding, and that the nature and purpose of business stay consistent with that provided by the customer as part of the onboarding and KYC process. Any significant changes should be documented and questioned. KYC information should also be reviewed periodically, based on risk or trigger events, such as a change of address.

Any customers that are deemed higher risk during onboarding or at any point during the CDD process should be subject to more frequent and thorough monitoring.

VASPs should also ensure that all documents and information submitted during onboarding are kept up to date throughout the course of the relationship.

Where customers require EDD, source and destination of funds identified during onboarding should continue to be queried throughout the course of the relationship.

Manual Vs Automatic Monitoring

Any transaction monitoring system aims to flag suspicious or unusual transactions and/or activities for further examination. Any flagged activities should be reviewed promptly and by the people with the appropriate training in this area, who then take the necessary steps in response to the findings, such as reporting to the relevant regulatory authorities and/or filing a suspicious transaction/activity report (STR/SAR). This can take place during the KYC process, when a transaction is initiated and is flagged, or after the transaction has taken place.

While manual monitoring and blockchain tracing is possible, the use of automated third-party blockchain analysis solutions is *highly* recommended. Blockchain analysis allows a more comprehensive understanding of any patterns of behaviour, as well as the ability to flag any criminal addresses and wallets. Risk ratings for customers are also significantly more nuanced when examined through blockchain analysis. Blockchain analysis should include both pre- and post-transaction wallet screening to identify source and destination of funds. Blockchain analysis and enhanced understanding of transaction patterns, as well as coordination with law enforcement, enables VASPs to quickly react to any hacks or stolen funds and freeze

them as appropriate, a technique that has been utilised previously in combating proliferation finance through VAs.

Case Study 4: 'Exchange 9' (2019)

The US Department of Justice unsealed a civil forfeiture complaint in August 2020 outlining the hacks of VASPs by North Korean actors, who laundered funds through Chinese over-the-counter markets.

The complaint states that in December 2019, one of the perpetrators attempted to convert stolen Ethereum to Bitcoin through a VASP (Exchange 9). The stolen Ethereum was hacked from a different VASP (Exchange 2), which had been publicised. As a result, Exchange 9 froze the funds involved in the transaction, as the stolen coins from Exchange 2 had been flagged in their system. The funds remain frozen in Exchange 9.

Source: US Department of Justice, 'United States Files Complaint to Forfeit 280 Cryptocurrency Accounts Tied to Hacks of Two Exchanges by North Korean Actors', 27 August 2020, <https://www.justice.gov/usao-dc/pr/united-states-files-complaint-forfeit-280-cryptocurrency-accounts-tied-hacks-two>, accessed 24 August 2021.

VASPs should not only invest in blockchain analytics but also in anti-money-laundering (AML) monitoring tools that look for classic transaction monitoring behaviours of ML/TF/PF.

Enhanced Due Diligence

Enhanced due diligence (EDD) should be carried out when a transaction or account is flagged as particularly high risk, or potentially suspicious. Particular high-risk indicators can be found in the next section. EDD relies on effective monitoring and should be applied on a risk-based system when financial crime activity is suspected. There are a variety of reasons why EDD might be necessary, including (but not limited to) when a customer:

- Is identified in a risk assessment as a particularly high risk for financial crime.
- Has an unnecessarily complex or opaque business structure.
- Transacts with individuals or entities in high-risk jurisdictions.
- Provides stolen or false identification during onboarding.
- Engages in transactions that do not match the nature and purpose of the relationship.
- Sends, receives or moves unusually large sums of virtual assets or fiat currency.
- Is a PEP.
- Cannot adequately explain the purpose of a transaction.

It is worth noting that the definition of 'large sums' of virtual assets is relative and will depend on the size of the VASP and the nature of the customer relationship.

If one or more of these concerns is identified, EDD should be initiated. The first step is to obtain additional identifying information. Some of this might be required from the customer, and some might be possible to ascertain separately via open sources. For a PEP, for example, title and details on the position held would be required.

An adverse/negative media check should also be undertaken to create a full profile. Overwhelmingly negative results to this check may indicate a customer with whom it is too high risk to continue a relationship.

Telephone or video interviews may also be necessary tools in understanding the nature and purpose of transactions.

Many VASPs also log IP addresses of customers as well as the location of any ATMs/banks/other VASPs involved in any exchange, to ensure that these locations match the expected relationship.

Virtual private networks (VPNs) may also be a risk indicator that could lead to EDD under specific circumstances. While there are legitimate uses for VPNs to create secure trading environments, there should be at least one touchpoint where a VPN is not active, such as registration with a VASP, in order for the VASP to log a genuine IP address.

VII. High-Risk Indicators and Red Flags

THERE ARE A number of high-risk indicators and red flags that may lead to EDD, STRs/SARs or even fund freezing. The FATF, the private sector and national regulators have all comprehensively listed identified red flags with corresponding case studies. Please see Annex I for more information.

Use of Mixers or Anonymising Services

Mixers, privacy wallets and CoinJoin[27] services all provide various types of transaction obfuscation and increase user privacy. Each obscures the transaction path and makes blockchain tracing increasingly difficult, and sometimes impossible.[28]

It is essential for VASPs to have the ability to identify transactions with mixers and privacy wallets, and treat transactions related to mixers as higher risk in most instances.

Such risk management might include:

- Creating an approved list of known and/or trusted mixers or CoinJoin services with whom customers are allowed to transact.
- Only allowing relationships with trusted mixers under specific conditions (under a certain value threshold).

Launderers and hackers working on behalf of proliferators have been known to use mixers increasingly frequently. The Lazarus Group in particular is known for its interest in and use of mixing services to obfuscate transaction trails.

27. CoinJoin is an anonymisation strategy that keeps cryptocurrency transactions private. It uses smart contracts to mix coins in new transactions, wherein the outputs are the same number of coins but are from a variety of different transactions, obfuscating the source and intended destination.
28. For more information on the specifics of these technologies, see Anton Moiseienko and Kayla Izenman, 'From Intention to Action: Next Steps in Preventing Criminal Abuse of Cryptocurrency', *RUSI Occasional Papers* (September 2019), pp. 19–24; Andrea O'Sullivan, 'What are Mixers and "Privacy Coins"?', Coin Center, 7 July 2020, <https://www.coincenter.org/education/advanced-topics/what-are-mixers-and-privacy-coins/>, accessed 24 August 2021.

Case Study 5: Lazarus Group (2018)

In their 2020 Crypto Crime Report, US-based blockchain tracing firm Chainalysis outlined the ways in which the Lazarus Group had changed its methods from 2019 to 2020. One of the areas highlighted was Lazarus's increased use of mixers and CoinJoin wallets.

According to Chainalysis, '48% of funds stolen by Lazarus moved to CoinJoin wallets' in 2019. In the DragonEx hack (Case Study 1), for example, Lazarus moved stolen altcoins such as Ethereum and Litecoin to VASPs, swapping them for Bitcoin. They then moved the Bitcoin to a series of local wallets before moving the funds to a Wasabi Wallet, which mixes the coins via the CoinJoin protocol.

While the 2021 Crypto Crime Report elaborates on other techniques being used by Lazarus, Chainalysis's statistics also show that Lazarus's use of mixers to launder stolen funds increased even further in 2020.

Source: Chainalysis, 'The 2020 State of Crypto Crime', January 2020, <https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf>, accessed 24 August 2021; Chainalysis, 'The 2021 State of Crypto Crime', 16 February 2021, <https://go.chainalysis.com/2021-Crypto-Crime-Report.html>, accessed 2 September 2021.

VIII. Reporting Requirements

REPORTING REQUIREMENTS AND filing of SARs/STRs may vary significantly between jurisdictions, while some jurisdictions may not yet require any reporting from VASPs. However, VASPs should be prepared to operate at the highest standard – alongside that of other regulated financial service providers – and should be fully aware of their jurisdiction's requirements. Staff should be required to report activity they find suspicious, and a clear process should be outlined, with staff reporting to the designated reporting officer who initiates an appropriate investigation and reports to the relevant authorities.

This process should be clearly outlined to staff. Relevant terms should be standardised and defined for ease of understanding on behalf of both the relevant financial intelligence unit and the VASP. Examples of reporting could include SARs/STRs filed due to:

- Concerns about the source of funds received into a user's wallet.
- Structured transactions in small amounts just under reporting thresholds.
- Immediate VA transfers to multiple VASPs operating in other jurisdictions, especially jurisdictions with weak VASP regulations.
- A user's wallet receiving funds from VA addresses that have previously been flagged in relation to stolen funds or ransomware.
- Forged or edited documents or photographs used for identification purposes.
- Inability of a VASP to obtain requested customer information, or a customer declining to provide CDD documents or source of funds information.

Please note that this is not an exhaustive list, and reporting should be undertaken whenever internal processes flag suspicious activity.[29]

29. The Cayman Islands Monetary Authority has published a list of further possible red flags that would trigger reporting requirements for VASPs in their jurisdiction. See Cayman Islands Monetary Authority, 'Guidance Notes (Amendments) on the Prevention and Detection of Money Laundering, Terrorist Financing, and Proliferation Financing in the Cayman Islands', February 2021, p. 13.

IX. Final Remarks

WHILE VASP COMPLIANCE and regulatory guidance has increased over the last few years, there is still considerable progress to be made. It is absolutely crucial that VASPs conduct risk assessments and a coordinated risk-based approach to ML/TF/PF activity.

The FATF expects countries to implement similar preventative measures for VASPs to those they require for traditional financial institutions, including appropriate supervision of the sector and licensing or registration requirements. While the FATF Recommendations are aimed at their member countries and not the VASPs themselves, country implementation of the Recommendations and Guidance has increasingly required VASPs to comply, and is expected to increase. VASPs have the opportunity now to understand what is required of the sector and proactively comply if their jurisdiction has not yet implemented the Recommendations.

There is also a considerable amount of debate regarding the FATF's Recommendation 16 on wire transfers, which advises VASPs to treat all VA transactions as cross-border transfers given the borderless nature of the technology.[30] This would require information sharing between VASPs to an unanticipated degree, including holding and sending both originator and beneficiary information to other VASPs involved in a transaction. There are currently a number of public and private organisations developing technological solutions to Recommendation 16.[31]

VASPs should be aiming for proactive compliance and be focused on a risk-based approach to effectively mitigate threats coming from proliferating countries aiming to exploit the system for their own gain.

As FATF risk assessment requirements are being amended to include PF, VASPs should be particularly vigilant for these types of actors. Case studies continue to indicate large-scale use of VAs for sanctions evasion, and more will surely be publicised in the future. To mitigate both business risk as well as the international and geopolitical risks of these actions, VASPs should apply the most comprehensive level of compliance possible, as illustrated in this guidance and the associated recommended readings (see Annex II).

---

30. FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations', p. 77.
31. For example, see Ian Allison, 'US Crypto Giants Build First Version of FATF-Compliant "Travel Rule" Tool', *CoinDesk*, 25 June 2021, <https://www.coindesk.com/us-crypto-giants-build-first-version-of-fatf-compliant-travel-rule-tool>, accessed 24 August 2021.

Annex I: Checklist

The checklist below summarises this guidance paper. For further elaboration regarding any of the steps, please refer to the appropriate section in the paper.

Pre-Requirements

- □ The virtual asset service provider (VASP) has a proper governance structure and compliance team.
    - o Senior management oversees and holds responsibility for the anti-financial crime programme.
    - o There is a Chief Compliance Officer (CCO).
    - o If applicable, there is a Sanctions Compliance Officer.
    - o Mid- and junior-level staff are briefed on all relevant compliance procedures that could manifest in other areas of the VASP's business.
    - o Staff are trained regularly on ML/TF/PF trends and typologies.
- □ The VASP has conducted at least one comprehensive, documented risk assessment in the last two years.
    - o The VASP has actioned key control requirements to address high areas of risk on the basis of the risk assessment outcomes.
- □ The VASP has effective cybersecurity protocols.
    - o Staff undergo regular cybersecurity training sessions.
    - o There is an appropriate and comprehensive IT and cybersecurity infrastructure in place.
- □ The VASP has appropriate asset listing requirements.

Sanctions and Politically Exposed Persons (PEP) Screening

- □ The VASP conducts sanctions screening for all customers.
- □ The VASP uses all available material to screen comprehensively.
    - o The VASP adheres fully to international and US sanctions lists.
    - o The VASP screens for actors included in UN Panel of Experts Reports.
    - o The VASP consults typology reports by NGOs and also uses negative media screening.
- □ The sanctions and PEP screening is ongoing. The VASP screens virtual asset (VA) wallets pre-transaction and conducts ongoing monitoring of transactions.
    - o Screening is conducted at first identity verification.
    - o Screening is conducted throughout the client relationship.

Onboarding

- □ The VASP has comprehensive know-your-customer (KYC) processes in place.
    - o Customer identification processes require, at a minimum, the customer's full name, date of birth, nationality and address.
    - o Customer personal information is verified using official government identification documents. Addresses are verified using a proof of address document or appropriate digital means.
    - o Legal entity identification requires, at a minimum, the entity's name, registration, address, status, identifying information of key management personnel, and ownership structure.
    - o Legal entity information is verified using the company number, relevant government registration documents, and registries.
    - o KYC and continual CDD processes are conducted on any beneficial owners or persons acting on behalf of the customer.

- Further KYC mechanisms are considered or implemented, including selfies taken within the app and video calls, verified by liveness tests.

- □ The VASP understands fully the nature and purpose of the customer relationship.
  - The customer provides expected frequency of transactions.
  - The customer provides expected size of transactions.
  - The customer provides expected volume of transactions.
- □ The VASP understands, to the extent possible, both the source and destination of any funds moved.

Ongoing Monitoring and CDD

- □ All documents and information submitted to the VASP during onboarding are kept up to date throughout the course of the relationship.
- □ The VASP has either a manual or automated transaction monitoring system in place.
  - The VASP uses a system that enables comprehensive sanctions screening.
  - The VASP understands the limitations of the system in place.
- □ The VASP has considered the benefits of implementing large-scale blockchain analysis.
- □ The VASP carries out enhanced due diligence (EDD) when a transaction or account is flagged as high risk.
  - The VASP understands when and how to conduct EDD.

High-Risk Indicators and Red Flags

- □ The VASP manages relationships with mixers.
  - The VASP creates an approved list of known and/or trusted mixers and CoinJoin services.

- The VASP only allows relationships with trusted mixers under specific conditions.

Reporting Requirements

- □ The VASP is aware of and understands the FATF Recommendations.
- □ The VASP is aware of, understands and complies with all appropriate jurisdictional regulation.
- □ The VASP is aware of, understands and complies with its jurisdiction's reporting requirements.
- □ A clear process is outlined for staff regarding how to report suspicious transactions and what specifically to send to the designated internal reporting officer.
- □ The designated reporting officer knows specifically how to report to the relevant authorities and escalate a situation.
- □ Relevant terms are internally standardised and defined for ease of understanding.

Annex II: Suggested Reading

FATF Guidance on Virtual Assets and Virtual Asset Service Providers

FATF, 'Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers', June 2019, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html>.

FATF, '12-Month Review: Virtual Assets and VASPs', July 2020, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html>.

FATF, 'Second 12-Month Review of Revised FATF Standards – Virtual Assets and VASPs', July 2021, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html>.

FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations', updated June 2021.

Guidance on Virtual Asset Service Provider Proliferation Financing Risk Assessment

Anagha Joshi, Emil Dall and Darya Dolzikova, 'Guide to Conducting a National Proliferation Financing Risk Assessment', RUSI, May 2019.

BitAML, 'Cryptocompliance 101: Do You Need a Risk Assessment? In Crypto, the Answer Is Yes', 28 January 2019, <https://bitaml.com/2019/01/28/risk-assessment-crypto/>.

FATF, 'Guidance on Proliferation Financing Risk Assessment and Mitigation', June 2021, <https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf>.

Government of the Grand Duchy of Luxembourg Ministry of Justice, 'ML/TF Vertical Risk Assessment: Virtual Asset Service Providers', December 2020, <https://mj.gouvernement.lu/dam-assets/dossiers/blanchiment/ML-TF-vertical-risk-assessment-on-VASPs.pdf>.

New Zealand Government Department of Internal Affairs, 'Financial Institutions Sector Risk Assessment', Part 19: Sector Risks – Virtual Asset Service Providers, December 2019, <https://static1.squarespace.com/static/5a77b9d390bade7aa2cf8692/t/600e144cc42d5b31a3ccc997/1611535442275/Financial-Institutions-SRA-2019.pdf>.

High-Risk Indicators and Red Flags

Chainalysis, 'The Chainalysis 2021 Crypto Crime Report', March 2021, <https://go.chainalysis.com/2021-Crypto-Crime-Report.html>.

Elliptic, 'Sanctions Compliance in Cryptocurrencies: Using Blockchain Analysis to Navigate the Minefield', May 2021, <https://www.elliptic.co/hubfs/downloads/Elliptic_Sanctions-Compliance-In_Crypto.pdf>.

FATF, 'Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing', September 2020, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf>.

Government of Canada Financial Transactions and Reports Analysis Centre of Canada (FinTRAC), 'Money Laundering and Terrorist Financing Indicators – Virtual Currency Transactions', December 2020, <https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/indicators-indicateurs/vc_mltf-eng>.

US Department of the Treasury, Financial Crimes Enforcement Network (FinCEN), 'Advisory on Illicit Activity Involving Convertible Virtual Currency', 9 May 2019, <https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf>.

Additional Sources for Sanctions Screening

Australian Government Department of Foreign Affairs and Trade Sanctions, 'Australia and Sanctions', <https://www.dfat.gov.au/international-relations/security/sanctions/consolidated-list>.

EU External Action Service, 'Consolidated List of Sanctions', <https://eeas.europa.eu/headquarters/headquarters-homepage_en/8442/Consolidated%20list%20of%20sanctions>.

Government of Canada, 'Consolidated Canadian Autonomous Sanctions List', <https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/consolidated-consolide.aspx?lang=eng>.

Japan Ministry of Economy, Trade and Industry, 'Sanctions List', <https://www.meti.go.jp/english/>.

UK HM Treasury Office of Financial Sanctions Implementation, 'Consolidated Sanctions List', <https://sanctionssearch.ofsi.hmtreasury.gov.uk/>.

UN Security Council, 'Consolidated List', <https://www.un.org/securitycouncil/content/un-sc-consolidated-list>.

UN Security Council, ‘Panel of Experts 1718 Sanctions Committee (DPRK) Reports’, <https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports>.

US Office of Foreign Assets Control, ‘Sanctions List Search’, <https://sanctionssearch.ofac.treas.gov/>.