FATF

FATF Report

Targeted Report on Stablecoins and Unhosted Wallets

Peer-to-Peer Transactions

March 2026

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

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

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

Citing reference:

FATF (2026), *Targeted Report on Stablecoins and Unhosted Wallets – Peer-to-Peer Transactions,* FATF, France, www.fatf-gafi.org/content/fatf-gafi/en/publications/virtualassets/targeted-report-stablecoins-unhosted-wallets

Table of Contents

Abbreviations and Acronyms **2**

Executive Summary **3**

Introduction **4**

Objectives and Structure 4
Previous FATF Work on Stablecoins 4
Scope 5
Methodology 5

Background **6**

Background on Stablecoin Ecosystem and Definitions 6
FATF Requirements for VASPs and Applicability to Stablecoins 8

Part One: Analysis on Current situation, Threats and Vulnerabilities **11**

Current Situation 11
Threat Actors Use of Stablecoins 12
Vulnerabilities 18

Part Two: Good Practices to Mitigate Misuse of Stablecoins, Including for P2P Transactions **22**

Effective Implementation of FATF Standards 22
Stablecoin Issuers Applying Controls 24
Using Advanced Tools for Detecting and Monitoring Suspicious Transactions 27
Effective Supervision of Stablecoin issuers and other entities involved in stablecoin arrangements 29
Robust Public-Private Sector Collaboration 31
Following Investigative Leads 32
ML/TF/PF Risks Mitigation measures for Unhosted Wallets and P2P Transactions 32

Conclusion **34**

Recommended Actions **35**

Annex A: List of Risk Indicators **37**

Abbreviations and Acronyms

AECs	Anonymity Enhanced Cryptocurrencies
AML/CFT/CPF	Anti-Money Laundering/Countering the Financing of Terrorism/Counter Proliferation Financing
CBDCs	Central Bank Digital Currencies
CDD	Customer Due Diligence
DeFi	Decentralised Finance
DEX	Decentralised Exchange
DLT	Distributed Ledger Technology
DPRK	Democratic People's Republic of Korea
DTOs	Drug trafficking organisations
EDD	Enhanced Due Diligence
FIs	Financial Institutions
KYC	Know Your Customer
ML/TF/PF	Money Laundering/Terrorist Financing/Proliferation Financing
OTC	Over the Counter
P2P	Peer to Peer
PPPs	Public–Private Partnerships
SAR/STR	Suspicious Activity/Transaction Report
TFS	Targeted Financial Sanctions
TRW	Travel Rule-covered Wallet
VAs/VASPs	Virtual Assets/Virtual Asset Service Providers

Executive Summary

1. Stablecoins have grown rapidly in scale, adoption, and functional integration within both the virtual asset ecosystem and, increasingly, the traditional financial system. As of mid-2025, over 250 stablecoins were in circulation, with total market capitalisation exceeding USD 300 billion and daily trading volumes surpassing those of Bitcoin. Fiat-backed, centrally governed stablecoins—predominantly USD-referenced—dominate the market and are widely used across multiple blockchains. While stablecoins are increasingly used for legitimate purposes, their distinctive features—price stability, high liquidity, interoperability—also make them attractive tools for threat actors.

2. Stablecoins, including through unhosted wallets, have become a common component of ML, TF and PF schemes that use virtual assets. While there are some simple and/or direct uses of stablecoins observed, many schemes use stablecoins as one feature in a more complex series of transactions designed to obfuscate the origin of funds, and distance it from the intended use. Reporting indicates that stablecoins are the most popular virtual asset used in illicit transactions.

3. Stablecoins, generally, have the same vulnerabilities as other virtual assets. These vulnerabilities are exacerbated by their characteristics such as the price stability and ample liquidity, which can make stablecoins more likely to be used in P2P transactions. P2P transactions via unhosted wallets represent a key vulnerability in the stablecoin ecosystem. Conducted without the involvement of AML/CFT-obliged intermediaries, these transactions can be of higher risk, especially when layered through unhosted wallets. In addition, stablecoins could exhibit more asset-specific vulnerabilities, notably those arising from their interconnections with traditional finance. Cases indicate that threat actors have used stablecoins to purchase prohibited goods without cashing out through intermediaries, however, data remains limited regarding the broader use of stablecoins for the purchase of goods and services or for P2P transactions. Therefore, it is important for jurisdictions and relevant stakeholders to continue to closely monitor whether stablecoins are increasingly used for purchases without reliance on traditional on- and off-ramps, and the extent to which accurate data on the scale and proportion of P2P transactions can be obtained.

4. In response to these risks and vulnerabilities, the report identifies a range of good practices that can be implemented by wider jurisdictions and private sector. Some are common with all virtual assets, while others unique to stablecoins. These include establishing comprehensive legal frameworks in compliance with the FATF Standards; imposing clear AML/CFT obligations on stablecoin issuers, intermediaries, and custodians; assessing risk and implementing risk mitigation measures for transactions involving unhosted wallets; and leveraging advanced technology-based tools. The report also emphasises the need for further coordination among competent authorities and across borders, as well as the importance of providing technical assistance to jurisdictions that have not yet adequately implemented regulatory and supervisory frameworks for stablecoins. This report also demonstrates several jurisdictions that have also adopted innovative approaches, such as requiring issuers to embed programmable controls in stablecoin smart contracts, to support freezing, deny-listing, or other risk mitigation actions in secondary markets.

5. Finally, this report makes available to members of the FATF Global Network indicators of the misuse of stablecoins, particularly through unhosted wallets. It also makes internal recommendations for the FATF Global Network to consider to potentially mitigate risk in the stablecoin environment.

Introduction

Objectives and Structure

6. Previous FATF work has focused on stablecoins more broadly[1]. The objective of this project is to enhance the understanding of emerging ML/TF/PF risks, threat actors and vulnerabilities related to stablecoins and unhosted wallets, particularly during P2P transactions. In addition, the project identifies and shares good practices to mitigate those risks.[2]

These objectives are achieved through three sections:

- **Background**: Sets out the various participants in the stablecoin ecosystem, provides relevant definitions, and outlines the applicability of the FATF Standards to stablecoins arrangements, as well as the current implementation status of FATF Standards.
- **Part One**: Analyses the current situation regarding stablecoin ecosystem development and how stablecoins differ from other virtual assets, and identifies threat actors as well as national and sectoral vulnerabilities exploited by them.
- **Part Two**: Explores good practices on mitigation measures from the public and private sectors, as well as on investigative and national/international co-operation.

Previous FATF Work on Stablecoins

7. The FATF has conducted work on stablecoins since 2019, first through the public study 'Money laundering risks from "stablecoins" and other emerging assets' and also the 'FATF Report to the G20 on So-called Stablecoins'.[3] The FATF continued to clarify the application of the FATF Standards to help jurisdictions mitigate those risks.[4] In the Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers (2025), the FATF observed that the use of stablecoins by a range of illicit actors, including DPRK actors, terrorist financiers, and drug trafficking networks, has continued to increase over time.[5]

8. The FATF has highlighted the need to closely monitor developments in the stablecoin ecosystem to ensure that the FATF Standards remain effective despite ongoing virtual asset evolution. In particular, the FATF underscored the importance of continued monitoring of: (1)

---

[1] 2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf;
Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers;
VIRTUAL ASSETS – DRAFT FATF REPORT TO G20 ON SO-CALLED STABLECOINS

[2] The FATF defines peer-to-peer (P2P) transactions as VA transfers conducted without the use or involvement of a VASP or other obliged entity (e.g., VA transfers between two unhosted wallets whose users are acting on their own behalf). See: Updated Guidance for a Risk-based Approach for Virtual Assets and Virtual Assets Service Providers

[3] FATF Money laundering risks from "stablecoins" and other emerging assets (2019); FATF (2020), FATF Report to the G20, FATF, France.

[4] FATF 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Assets Service Providers (2021); FATF Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers (2021); FATF Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Assets Service Providers (2021).

[5] FATF Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers (2025).

whether stablecoins achieve global mass adoption in a manner that allows the purchase of goods and services with little or no reliance on traditional on- and off-ramps; and (2) the extent to which jurisdictions and the private sector are able to obtain accurate data on the scale and proportion of P2P transactions.

Scope

9. This report reflects developments in the stablecoin ecosystem until the end of 2025. It explains the applicability of the FATF Standards to the various participants involved in stablecoin arrangements, identifies the market development of stablecoins, shows the increasing ML/TF/PF risks of stablecoins, particularly associated with unhosted wallets during P2P transactions.

10. The report explores the vulnerabilities of stablecoins, some of which are common to most virtual assets, while others are unique to stablecoins. The report focuses on providing practical risk mitigation measures for stablecoins, with a focus on P2P transactions with a variety of case studies provided by jurisdictions, concluded by recommended actions for relevant stakeholders. As with all FATF guidance products, the Guidance is non-binding.

Methodology

11. The methodology involved collecting and analysing inputs from the FATF project team and the Virtual Asset Contact Group (VACG) members, engaging with relevant stakeholders, and reviewing and refining existing materials on stablecoin arrangements, including:

- Two rounds of requests for information were made to the FATF project team and VACG members to provide inputs. These requests yielded (a) 29 case studies on threats, typologies, and jurisdictional measures were received, and (b) 25 inputs were submitted on AML/CFT/CPF obligations of participants in the stablecoin ecosystem, regulatory challenges, and good practices for mitigation measures.
- Private sector entities, such as stablecoin issuers and blockchain analytics companies, were invited to respond to a targeted outreach survey focusing on challenges and good practices in mitigating illicit finance risks associated with stablecoins.
- A virtual roundtable meeting with key stakeholders was held based on the survey results to gain more detailed insights on mitigation measures.

Background

Background on Stablecoin Ecosystem and Definitions

Basic Definitions

12. A stablecoin is one form of virtual assets, which is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. While the FATF has recognised that stablecoins are not a legal or technical category and clarified that the use of this term by the FATF is not intended to endorse any stability claims, the term generally refers to a type of virtual asset that has a stabilisation mechanism and can be used as a means of payment and/or store of value.[6] Often, stablecoin seeks or purports to maintain price stability by linking its value to one or more reference assets, such as fiat currencies or virtual assets, and may be backed by such assets. Regardless of how stablecoins are considered at national level, providers of services to stablecoins who fit the FATF definition of VASP or FI should be subject to the corresponding obligations in accordance with the FATF Standards.[7]

Asset-Backed Stablecoins

13. Asset-backed stablecoins are backed by financial assets such as fiat currencies or government bonds. Issuers of asset-backed stablecoins often purport and commit to have the ability to redeem stablecoins for the backing asset on a 1:1 basis for users at all times, which could contribute to price stability. Asset-backed stablecoins in general have centralised governance structures, often managed by the issuer.

VA-Backed Stablecoins

14. VA-backed stablecoins are issued using virtual assets (VAs) and tokenised financial instruments as collateral. Due to concerns over the price volatility of the collateral assets, such arrangements typically require and maintain an over collateralised position. Issuance, redemption, collateral management and liquidation are often conducted through autonomous smart contracts, and in some cases, users may be able to issue stablecoins directly without relying on centralised governing entities.

Algorithmic Stablecoins

15. Algorithmic stablecoins are typically designed to maintain price stability by adjusting supply through smart contracts or algorithms such as synthetically collateralised dollar-type stablecoins[8] without any backed assets. Algorithms managing the economics of the stablecoin increase supply when prices rise and decrease supply when prices fall to maintain stability. Issuance and management are often conducted through autonomous smart contracts, and governance can be more decentralised than with asset-backed stablecoins. Generally, these stablecoins do not offer redemption into fiat currency, and instead aim to stabilise prices through mechanisms such as stablecoin swaps or burns.

---

[6] Financial Stability Board, High-level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangements: Final report.

[7] FATF (2021) Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers

[8] These stablecoins incorporate mechanisms that offset price volatility by combining virtual assets with derivatives.

Participants in the Stablecoin Ecosystem

16. There are various participants in the stablecoin ecosystem. Relevant participants and their roles can differ depending on the organisation and nature of stablecoins and their arrangements.

- **Stablecoin Issuers**: Stablecoin issuers are responsible for issuing and redeeming stablecoins and ensuring their purported stability in the interim. They often mint stablecoins in exchange for fiat currencies or other assets while collecting fees for issuance and redemption. In many cases, the issuer also deploys and maintains the smart contracts necessary for all on-chain transactions in their stablecoin. Moreover, the issuer can assign part of its functions, such as redemption, to intermediary VASPs.
- **Reserve Custodians**: Reserve custodians store and manage the reserve assets backing the stablecoins on behalf of the issuer.
- **Intermediaries**: VASPs including VA exchanges and financial institutions that provide buying, selling, safekeeping, trading or conversion services for stablecoins. Some exchanges may buy stablecoins from the issuer and distribute them into the retail market. Decentralised finance (DeFi) may also provide services to users, such as remittance, payment, exchange, and lending involving stablecoins.
- **Payment Service Providers/Card Networks**: Payment service providers and card networks can enable the use of stablecoins for payments for goods and services by offering stablecoin payment infrastructure to merchants. They can also facilitate remittances to individuals.
- **Unhosted Wallets:** Virtual asset wallets that are not hosted or managed by a third-party service provider and where the user maintains exclusive control over the access keys. Certain unhosted wallet service providers also offer stablecoin swap functions.
- **Blockchain Analytics Tool Providers**: Blockchain analytics tool providers generate analysis based on information obtained from examination of blockchains and entities with customer interfaces, such as wallet service providers, and this data may be utilised by stablecoin issuers and intermediaries to support measures to mitigate illicit finance risk including restrictive measures requirements. They use different taxonomies, which make the outcomes of their analysis difficult to compare.

Stablecoin Lifecyle and Features

17. A stablecoin issuer typically issues stablecoins and they are circulated amongst users and VASPs and then redeemed for fiat currency. While the mechanisms for issuance and redemption vary depending on the type of stablecoin, this section provides the general processes in this lifecycle for centrally issued asset-backed stablecoins.

18. Stablecoin issuers typically issue stablecoins by receiving fiat currencies or VAs from contracting parties and minting stablecoins corresponding to the value received. Issuing a stablecoin creates two types of markets:

- **Primary**: Primary customers purchase or redeem stablecoins directly from the issuer and then could put the stablecoin into broader circulation in the secondary market. These customers, typically VASPs or institutional clients, undergo customer due diligence and onboarding procedures. They can also be retail customers.
- **Secondary**: Secondary customer stablecoin holders may use a hosted wallet involving a VASP or financial institution subject to AML/CFT obligations, or use unhosted wallets to hold and transfer the stablecoins peer-to-peer, without the involvement of an AML/CFT obliged entity. Accordingly, secondary customers using unhosted wallets may not be subject to AML/CFT obligations.

19. Stablecoin issuers often maintain a degree of control over their stablecoins in both primary and secondary market transactions using smart contracts. Issuers can program smart contracts to prevent certain wallet addresses from transacting in their stablecoin (e.g., black-listing) or to remove stablecoins from circulation in the secondary markets (*i.e.*, freezing or burning). Issuers can also view all on-chain transactions in their stablecoin given the nature of public blockchains.

20. Typically, redemption from the issuer is available only to primary customers, subject to the issuer's rules. In some cases, redemption may be facilitated through issuer-designated intermediaries in accordance with applicable legal frameworks. Primary and secondary stablecoin holders may exchange stablecoins for fiat currency or other virtual assets through centralised intermediaries (VASPs), decentralised exchanges (DEXs), or via peer-to-peer transactions.

Governance Structure

21. Generally, stablecoin arrangements have a governing structure that is responsible for the operation of the stablecoin services. A centralised governance body such as issuers and intermediaries may perform the core functions of the stablecoin arrangement (such as AML/CFT/CPF and managing stabilisation mechanisms). In many existing arrangements, the issuer takes on the key role of governing the stablecoin arrangement, although some functions could be managed by intermediaries or technology providers. Stablecoin arrangements can also be structured in a decentralised manner as discussed in previous sections, which can make responsibility ambiguous.

FATF Requirements for VASPs and Applicability to Stablecoins

22. FATF Recommendation 15 of the FATF Standards requires all jurisdictions to:[9]

a. identify, assess and understand the ML/TF/PF risks emerging from VAs and VASPs.

b. ensure that VASPs are required to be licensed or registered in the jurisdiction where they are created.

c. apply sanctions to natural or legal persons that carry out VASP activities without the requisite license or registration.

[9] See the Interpretative Note of Recommendation 15, FATF Recommendations www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf

d. ensure that VASPs are subject to supervision.

e. apply proportionate and dissuasive sanctions to VASPs that fail to comply with AML/CFT/CPF requirements.

f. ensure that targeted financial sanctions obligations apply to VASPs.

23. VAs are defined by the FATF as a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations. Given their characteristics, the FATF considers stablecoins as virtual assets.

24. Persons and entities involved in stablecoin arrangements would be classified as VASPs or FIs in the circumstances detailed below[10]:

- **Stablecoin Issuers**: Under the FATF Standards, the sole act of issuing a VA on its own is not a covered service under the definition of VASP. However, stablecoin issuers[11] who as a business conduct one of the following activities fall within the FATF definition of VASP[12] or FI[13]: 1) engage in exchange or transfer activities, such as exchanging customer's fiat currencies/VAs for their stablecoins during the issuance or redemption process or; 2) participate in and provide financial services related to an issuer's offer and/or sale of a virtual asset.[14]
- **Intermediaries**: Intermediaries involved in exchanging stablecoins for fiat currency or virtual assets, transferring stablecoins or providing safekeeping and/or administration services for stablecoins fall under the FATF definition of VASP. Such intermediaries can include exchanges, trading platforms, custodial wallet providers, certain types of unhosted wallet service providers, and over-the-counter brokers. Unhosted wallets that engage in, or actively facilitate as a

[10] See the 2021 FATF Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers; the FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins; FATF, Money laundering risks from "stablecoins" and other emerging assets, October 2019.

[11] The definition includes natural and legal persons.

[12] According to the FATF 2021 updated guidance, the sole act of issuing a VA, entirely on its own, is not a covered service under limb (v) of the VASP definition. However, any persons which conduct the exchange and transfer of the issued VAs as a business for or on behalf of another person would be a covered service, as would the participation in and the provision of financial services related to any ICO associated with the issuance.

[13] According to the FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins, the FATF considers that these developers and governance bodies will be, in general, financial institutions (e.g., as a business involved in the 'issuing and managing means of payment') or a VASP (e.g., as a business involved in the 'participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset') under the revised FATF Standards.

[14] According to the FATF 2021 updated guidance, the sole act of issuing a VA on its own is not a covered service under limb (v) of the VASP definition. However, the FATF Standards apply to activities related to ICOs (see: page 30, 2021 FATF Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers)

business, any VA activities or operations covered by Recommendation 15, for or on behalf of another person, should be regulated as VASPs.[15]

- **DeFi Arrangements**: Creators, owners, operators and other persons who maintain control or sufficient influence in the DeFi arrangements, even if those arrangements seem decentralised, may fall under the FATF definition of VASP where they are providing or actively facilitating VASP services. Where it has not been possible to identify a legal or natural person with control or sufficient influence over a DeFi arrangement, there may not be a central owner/operator that meets the definition of a VASP. However, many DeFi arrangements in practice are decentralised in name only.

25. The FATF does not consider natural or legal persons that provide ancillary services or products to a VA network to be VASPs. This includes the provision of ancillary services like hardware wallet manufacturers or providers of unhosted wallets, to the extent that they do not also engage in VASP activities. P2P transactions via unhosted wallets are not explicitly subject to AML/CFT controls under the FATF Standards as obligations are generally placed on intermediaries rather than on individuals.[16]

[15] Paragraph 83, Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers

[16] With some exceptions, such as requirements related to implementing targeted financial sanctions.

Part One:
Analysis on Current situation, Threats and Vulnerabilities

Current Situation

26. The first stablecoin that was promoted as pegged 1:1 to the US dollar appeared in 2014. Since then, the number of circulating stablecoins has skyrocketed, with 259 circulating stablecoins as of the end of June 2025.[17] The market capitalisation and trading volume of stablecoins have also grown substantially. Stablecoin market capitalisation reached USD 316 billion in October 2025, representing approximately 8% of the total market capitalisation of virtual assets. At the same time, the 24-hour trading volume reached USD 156 billion, almost three times that of the USD 55 billion for Bitcoin. Overall, stablecoins represent 30% of all on-chain virtual asset transaction volume in 2025.[18]

27. Within the stablecoin market, fiat currency-backed stablecoins dominate, representing 95% of the total market capitalisation in October 2025. Of this, USD fiat-currency backed stablecoins account for 97% of the currency-backed stablecoins. Virtual asset-backed stablecoins account for 3% of overall stablecoin activity and algorithmic stablecoins only 0.2%. As of mid-2025, 90% of stablecoins were centralised.

28. There are multiple reasons behind increased adoption in stablecoins. Financial institutions, VASPs, and retail users are attracted to the potential advantages of stablecoin transactions, including faster settlement times, lower transaction fees, cross-border capabilities, and lack of reliance on traditional business operating hours. In some cases, financial institutions are increasingly accepting stablecoins for payments. Some users are attracted to stablecoins for their store of value and therefore individuals in countries with weak or unstable currencies are using stablecoins. Analysis from the European Systemic Risk Board questions the volume of stablecoins used for payments and instead posits that stablecoins' market capitalisation is driven by trading volume of unbacked virtual assets. As large jurisdictions establish or clarify applicable regulatory frameworks, institutional interest in stablecoins has grown significantly over the last couple of years, with banks, card networks, money transmitters, large technology companies, and others expressing interest in entering the stablecoin ecosystem.[19]

---

[17] Stablecoins & CBDCs Report - June 2025

[18] www.trmlabs.com/reports-and-whitepapers/2025-crypto-adoption-and-stablecoin-usage-report

[19] The FATF, the International Monetary Fund, the Financial Stability Board (FSB), together with Standard-Setting bodies support and promote a global coordinated policy and regulatory approach to virtual assets and stablecoins. The G20 virtual asset implementation roadmap status report highlights that nearly all FSB member jurisdictions have already regulatory frameworks for virtual assets and stablecoins in place, or have plans in place to revise them or to develop new ones; Thematic Review on FSB Global Regulatory Framework for Virtual asset Activities: Peer review report

Threat Actors Use of Stablecoins

29. Stablecoins are increasingly used for ML, TF and PF. Chainalysis indicates that stablecoins accounted for 84 percent of the USD $154B illicit virtual asset transaction volume in 2025, surpassing Bitcoin as the dominant asset for cybercrime-related on-chain transactions.[20] [21] Some of the characteristics that make stablecoins appealing for legitimate users also attract criminals to misuse stablecoins for money laundering, terrorism financing, sanctions evasion, and proliferation financing. Compared to more volatile assets such as Bitcoin (BTC) or Ether (ETH), stablecoins like USDT (Tether) and USDC (Circle) offer a relatively stable medium for moving proceeds. Stablecoins have also become increasingly attractive to threat actors due to their liquidity, interoperability, and ease of cross-border transfer.

30. Threat actors increasingly favour the use of stablecoins across multiple blockchains including Aptos, Avalanche, Ethereum, Solana, and Tron. The majority of illicit activity in stablecoins occurs in the secondary market.

31. While the specific techniques differ by crime or group, common themes include use of unlicensed or unregistered VASPs, which are often located in jurisdictions without AM-L/CFT controls for VASPs, or VASPs that fail to comply with AML/CFT obligations, often over the counter (OTC) brokers or peer-to-peer platforms. Threat actors also use obfuscation techniques and services, like mixers and chain hopping. Stablecoins are used at various points in a longer transaction process, including being received as proceeds from the predicate crime or in the last leg to convert illicit virtual assets into fiat currency.

32. Some threat actors, such as terrorist financiers or drug traffickers, abuse stablecoins, and other virtual assets, as one method to raise and move money, but also still rely on more traditional methods. Other threat actors, specifically DPRK, rely on virtual assets and specifically leverage stablecoins as part of the laundering and cash out process. In general, any threat actor that abuses virtual assets and leverages unlicensed OTC brokers to cash-out to fiat, relies on stablecoins as OTC brokers typically demand stablecoins.

DPRK and Iran Proliferation Financing

33. State-linked cybercriminal groups have rapidly adopted stablecoins as a preferred method for laundering proceeds from ransomware, phishing, and other cyber-enabled crimes. Most notably, DPRK's Lazarus Group, Andariel, and Onyx Sleet specialise in virtual asset theft, espionage, and disruptive attacks, like ransomware. In particular, DPRK state-sponsored groups like Lazarus have used malware and social engineering to infiltrate virtual asset firms to steal funds, including a nearly $1.46 billion theft in February 2025. In this example, DPRK actors laundered the stolen funds through mixers, cross-chain bridges, and over 125,000 Ethereum wallets, indicating quick, high-volume transactions likely intended to complicate tracing. DPRK also uses decentralised exchanges (DEXs) and occasionally anonymity-enhanced cryptocurrencies (AECs) in the laundering process. DPRK launderers often convert laundered funds into stablecoins, often USDT on the Tron blockchain, before exchanging them into fiat currency through OTC brokers or peer-to-peer platforms.

34. According to the MSMT, since at least 2023, the DPRK's 221 General Bureau has sought to expand the use of stablecoins beyond cyber-enabled financial crime to include their use as a means of exchange and payment for goods and services prohibited under UNSCRs.[22] The 221 General Bureau is assessed by the MSMT to function as the DPRK's primary weapons trading

[20] 2026 Crypto Crime Report Introduction - Chainalysis
[21] Stablecoins dominate illicit crypto activities, eclipsing Bitcoin
[22] MSMT(Multilateral Sanctions Monitoring Team)

organisation and is designated by the UN under its former name, the Korea Mining Development Trading Corporation (KOMID). In particular, DPRK entities have been assessed to use Tether (USDT) in transactions involving the sale and transfer of military equipment and raw materials, such as copper used in munitions production. This activity indicates an apparent effort by DPRK entities to operationalise the use of stablecoins in WMD-related procurement activities.

35. The ability to conduct transactions using stablecoins such as USDT for prohibited activities provides UN-designated DPRK entities with an additional mechanism to evade international sanctions. Compared to cash-based transactions—which often require physical transportation across borders—payments made and accepted in USDT are less logistically burdensome, faster, and potentially lower-risk, thereby facilitating procurement activities prohibited under relevant UN Security Council resolutions.

36. In addition, Iranian actors are leveraging stablecoins to finance proliferation. Notably, the Islamic Revolutionary Guard Corps (IRGC) has turned to virtual assets to finance its evasion activities, with blockchain analytics companies assessing that several billion dollars in funds were received by IRGC-associated addresses on-chain in 2024 and 2025. UN sanctioned Iranian actors use virtual assets to obtain drone components and other high-tech equipment, and Iran has begun accepting virtual assets for weapons payments. Iranian actors have also been assessed to use virtual assets to transfer funds to UN sanctioned actors in the region, such as the Houthis, for weapons procurement. Stablecoins are often the virtual assets preferred by Iranian illicit actors for these transactions due to stablecoins' superior ability to finance international trade. Iran is adapting in response to disruptions to ensure sanctioned actors can continue to evade UN sanctions. For instance, freezes of USDT for IRGC-linked addresses in mid-2025 may encourage sanctioned Iranian entities to move towards other stablecoins, such as DAI, that do not have a freeze function.[23]

Money Laundering

37. Money launderers and perpetrators have been observed to use stablecoins to collect proceeds involving investment fraud, impersonation fraud, romance scams, pig butchering, and sextortion. Perpetrators may request funds in a variety of virtual assets, most commonly bitcoin or stablecoins, and may also use stablecoins in the laundering process. Their laundering process has been observed to involve the use of VASP services that may be unregulated in certain jurisdictions or fail to comply with regulatory obligations, and may include the use of mixers, DEXs, coin-swap platforms, and peer-to-peer platforms. These services often intersect with unregistered or unlicensed VASPs including OTC brokers to exchange stablecoins for fiat currency, completing the money laundering cycle.

[23] Iran's Crypto Economy in 2025: Declining Volumes, Rising Tensions, and Shifting Trust | TRM Blog

Box 1. Case Study: Use of online gambling platforms

A series of transactions were detected involving funds originating from online casinos using virtual assets. The funds were rapidly converted into stablecoins using a custodian wallet hosted by a VASP operating in France. Following these transfers, the stablecoins were converted into fiat currency and deposited into several bank accounts. The VASP filed an STR to TracFin, the French FIU.

Several red flags were identified by the VASP related to the misuse of online gambling platforms and stablecoins, including use of online casinos by individuals whose gambling activity appeared inconsistent with their customer profile or declared source of funds. Additionally, the rapid conversion of gambling winnings into stablecoins without economic purposes suggests an attempt to obfuscate the source of funds.

Source: France

38. Drug trafficking organisations are increasingly leveraging the use of stablecoins, particularly USDT on TRON and USDC on Ethereum, for paying overseas suppliers of synthetic drug precursors, settling drug transactions and laundering proceeds of drug trafficking. For procurement, transferred stablecoins are quickly converted into local currency or reinvested into further drug production. The laundering schemes often involve the use of money mules, OTC brokers and peer-to-peer platforms, and rapid virtual asset transactions across multiple blockchains, complicating detection and disruption efforts by law enforcement and financial intelligence units. Drug trafficking organisations also exploit high-volume online gambling platforms and merchant refund loops, where goods are purchased using stolen identities and returned for refunds in stablecoins to third-party wallets. Similar to the laundering of fraud proceeds, drug trafficking proceeds are often exchanged for fiat currency via unlicensed or unregistered VASPs, including OTC brokers, in jurisdictions with weak or non-existent AML/CFT controls.

Box 2. Case Study: Cross-Border Drug Trafficking Proceeds Laundered via Stablecoins

An organised crime network was suspected of laundering the proceeds of drug trafficking by purchasing Ether (ETH) at a regulated Virtual Asset Service Provider (VASP). The ETH was swapped for USDT (Tether) and USDC (Circle) on decentralised exchanges (DEXs) and coin-swap platforms without Know Your Customer (KYC) checks. The USDT and USDC were transferred to wallets controlled by a shell import–export company in Canada. Funds were layered through multiple wallets and eventually off ramped via OTC brokers and regulated VASPs. In other instances, fiat currency off ramped from a regulated VASP was wired to the criminals' domestic bank accounts as "investment proceeds." The FIU's financial intelligence disclosures and strategic analysis enabled law enforcement to trace the proceeds of drug trafficking and identify the organised crime financial network and tradecraft.

Source: Canada

39. Professional money launderers employ sophisticated layering techniques using stablecoins, including chain-hopping, smurfing (breaking transactions into smaller amounts), and cross-chain transfers to obscure the origin and destination of funds. Similar to the process of laundering proceeds from fraud, scams, and drug trafficking, professional money launderers also often use unregulated or unlicensed VASPs or VASPs that fail to comply with AML/CFT obligations. They also use DEXs that lack know your customer protocols, virtual asset automated teller machines (ATMs), and online gambling platforms, which can further complicate tracing efforts. Additionally, in some cases, stablecoins are used to settle transactions in underground banking arrangements.

Box 3. Case Study: Remuneration of trafficked humans in Southeast Asia through a Southeast Asia–based payment service provider

An Operational Analysis was carried out by FIU India in the case of set of persons receiving VDA Deposits from a Southeast Asia–based payment service provider. An Indian Virtual Digital Asset Service Provider (VDA SP) identified a pattern among a set of customers whose IP addresses were traced back to Southeast Asia. These individuals exhibited a consistent behavior of funding their accounts with USDT, immediately liquidating it, and withdrawing the corresponding amount in INR to their bank accounts and with no other types of transactions apart from this.

As a part of EDD, Virtual Digital Asset Service Provider (VDA SP) tried to reach out to the mobile numbers of customers, they were either switched off or not reachable. Since these customers were not reachable over phone, Virtual Digital Asset Service Provider (VDA SP) made attempts to reach out through a messaging platform. After repeated attempts, VDA SP was able to connect with 21 customers and it was found that the customers were in various locations in Southeast Asia and were employed as construction labor, restaurant workers etc. Several customers were also having same device fingerprint i.e., have logged in from the same device and various users shared the same IP at the time of making of VDA Transactions.

It was thus found that Indians working in scam centres in Southeast Asia (Mainly in Cambodia and Myanmar) are using a Southeast Asia–based payment service provider for transfer of salary (paid in cash in Thai Baht or USD) to their family, friends and relatives in India. Six users of the VDA SP were found in the list of unreturned Indian passengers from Southeast Asia. These passengers had gone on visitor visa and have not returned in 3 months. 241 user locations shared were found to be in and around the scam compounds operating in Cambodia. New scam compound locations were also identified.

Further, in the month of October 2025, compliance action was initiated and notice under Section 13 of Prevention of Money Laundering Act 2002 was issued by FIU India against a Southeast Asia–based payment service provider which was found to be illegally operating in India. Operations of the entity were further blocked in Indian Jurisdiction.

Source: India

Terrorist Financing

40. Terrorist organisations using virtual assets increasingly favour stablecoins over Bitcoin for reasons similar to those identified for money launderers. Terrorist organisations ISIL (Da'esh) and its regional affiliates and Al-Qaeda have been reported to solicit donations in stablecoins via encrypted platforms and social media and to use stablecoins to transfer funds within the group. They provide rotating wallet addresses to receive virtual assets, including stablecoins, from supporters worldwide to obfuscate the recipients of the transfers. They have also been observed to use stablecoins to break down larger sums into many small transfers that pass through multiple VASPs to lower the risk of detection.

41. As noted in the FATF 2025 Comprehensive Update on Terrorist Financing Risks, virtual assets are more often used in combination with more traditional TF methods. For example, a fundraising campaign may be established on a dedicated crowdfunding platform, shared through social media, and collect payments in VAs. Following a crowdfunding campaign, terrorist entities and facilitators use various offline and online means to manage and move funds, including HOSSPs.

42. Terrorist financiers are increasingly observed pairing stablecoin assets with decentralised finance aggregators, coin-swap exchanges, anonymity-enhancing tools, and unhosted wallets to circumvent compliance controls. Their campaigns have been observed to leverage recycled QR codes, domains, and change addresses allowing financing operations to persist despite enforcement takedowns. Transaction patterns typically feature dense multi-hop transfers, micro-splitting of funds, and re-aggregation before off-ramping, often through OTC brokers that advertise minimal or no CDD requirements. These tactics enable sanctioned or designated networks to obscure the origin and intent of funds while accessing global liquidity pools, posing significant challenges to financial intelligence and regulatory enforcement.

Box 4. Case Study: Detection of a case of terrorism financing involving stablecoins

In early 2025, a VASP operating in France detected irregular patterns of transactions involving a retail customer. Over several weeks, the customer had initiated regular outbound transfers of stablecoins to a specific external wallet. These transactions were small in value, frequent, and lacked a legitimate commercial or personal rationale raising initial red flags.

The recipient of the funds was suspected to be part of a terrorist organisation. Blockchain analysis revealed that the receiving wallet had direct exposure to previously sanctioned addresses linked to terrorism financing networks. The sender appeared to be acting as a facilitator. The pattern suggested purposeful structuring (smurfing) to avoid detection thresholds and monitoring protocols.

The suspicious activity was detected through blockchain analytics tools. The VASP in question used on-chain analysis tools capable of tracking wallet exposure to high-risk entities. The tools flagged the receiving wallet as having direct links to multiple addresses previously involved in terrorism financing cases. A STR was filed to TracFin, the FIU and included full transactional details, blockchain links, and customer identification data.

Source: France

Vulnerabilities

Vulnerabilities Across the Stablecoins Value Chain and Lifecycle (Issuance, Circulation, Redemption)

Issuance

43. The inherently borderless nature of stablecoin activities may create incentives for stablecoin issuers to establish their headquarters in jurisdictions with weaker regulatory frameworks while operating on a cross-border basis. As a result, stablecoin issuers—including offshore-based and decentralised entities—could pose challenges for competent authorities in terms of effective monitoring and supervision, in ways similar to those observed with other offshore VASPs. The risks associated with offshore VASP activities, including regulatory arbitrage and supervisory blind spots, are further examined in the FATF paper 'Understanding and Mitigating the Risks of Offshore VASPs'.

44. In addition, multi-issuance stablecoin schemes pose potential financial crime risks. Multi-issuance schemes involve an entity from jurisdiction A jointly issuing a stablecoin with an entity from jurisdiction B, resulting in the issued stablecoins being fungible and indistinguishable across the two entities. These arrangements may hinder the activity of LEAs, especially tracing, freezing or seizing of stablecoins, since two or more stablecoin issuers based in different jurisdictions are involved. Another key challenge for Supervisors and LEAs would be ensuring effective AML/CFT control and obtaining customer information, since it may be difficult to determine clear compliance responsibilities among issuers which might comply with different AML/CFT requirements. In addition, geolocation is complicated by the use of VPNs, and therefore it may be difficult to determine which entity maintains relevant information and responsibilities.

Circulation

45. The integrity of the stablecoin ecosystem depends on the regulation of intermediary VASPs, thorough implementation of AML/CFT measures. A key challenge is that compliance levels vary greatly across stablecoin ecosystem participants, with some intermediary VASPs operating more sophisticated compliance frameworks, for example, using blockchain analytics tools, while others have under-resourced or weaker compliance programs. Intermediary VASPs located in jurisdictions that have not implemented Recommendation 15 may have no compliance programs at all, creating a critical loophole in the global stablecoin regulatory framework.

Redemption

46. Redemption refers to the conversion of stablecoins back into fiat currency or the relevant backing asset. The FATF requires that VASPs and financial institutions providing redemption services apply AML/CFT measures on the ultimate beneficiaries of the assets. Regulated VASPs and financial institutions exchanging stablecoins for the backing asset must collect customer information, conduct sanctions screening, and comply with the Travel Rule (where applicable) along with other compliance obligations. Redemptions conducted through compliant VASPs or financial institutions should therefore be subject to effective supervision with appropriate information available to competent authorities.

47. A key vulnerability in the redemption stage is that stablecoin holders do not necessarily need to use official redemption channels to convert stablecoins into fiat currency. Although exchange activity in the secondary market does not constitute redemption in a technical sense,

stablecoins can be exchanged for fiat currency or backing assets via informal channels or non-compliant service providers, including OTC brokers or peer-to-peer platforms that operate without a licensed or registered intermediary. This creates opportunities for criminals to bypass formal controls and obtain assets that can be reinvested or used outside the virtual asset ecosystem. Jurisdictions should actively identify and monitor these unofficial and unregulated exchange mechanisms that have redemption-effecting outcomes, as they represent a critical loophole.

P2P Transactions via Unhosted Wallets

48. P2P transfers via unhosted wallets (P2P transactions) present illicit finance risks that may not necessarily be mitigated by the AML/CFT/CPF framework for the stablecoin ecosystem. These transactions occur directly between individuals or entities, without the involvement of a regulated intermediary VASP or FI and therefore fall outside AML/CFT/CPF obligations, making them inherently of higher risk.

49. FATF has previously conducted market metric analysis on P2P transactions but was unable to present definitive figures due to significant discrepancies in data among companies[24]. While analysing the size of the P2P sector remains challenging, it is critical that jurisdictions continue to monitor P2P and unhosted wallets-related risks.

50. To address this gap, the FATF Guidance for a Risk-Based Approach to VAs and VASPs makes clear that VASPs should collect the required originator and beneficiary information even when conducting a transfer between their customer and an unhosted wallet. Jurisdictions that allow VASPs to undertake transfers with unhosted wallets should assess the risks and implement commensurate risk mitigation measures.[25]

51. Notwithstanding the FATF's approach, threat actors may still transfer stablecoins through the use of layered unhosted wallets that are transactionally distant from Travel Rule-covered wallet (TRW). The ML/TF/PF risks of these transactions can be further aggravated when such transactions are conducted on a cross-border basis. Due to the near-instant settlement of stablecoins to recipient addresses located outside the originating jurisdiction, competent authorities may face increased difficulty in monitoring and tracing such transfers.

52. While P2P transactions on public blockchains remain visible and traceable, the transaction information is inherently pseudonymous, allowing criminals to exploit higher levels of pseudonymity to obscure attribution and conceal their identities from competent authorities. Such obfuscation risks are further exacerbated where criminals frequently generate new wallet addresses and abandon previously used ones. The proliferation of newly created addresses can complicate the ability of competent authorities to assess whether P2P transactions are linked to criminal activity or sanctioned entities.

53. Another structural limitation of the AML/CFT framework in relation to P2P transactions via unhosted wallets concerns the reporting of suspicious transactions, given the absence of an obliged entity responsible for submitting STR in respect of such transactions. While VASPs may implement robust Travel Rule requirements in relation to transactions involving their customers' unhosted wallets, including monitoring such transactions and reporting STR to the FIU, they may have limited visibility over, and therefore limited ability to monitor or report,

[24] FATF(2021) Second 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs

[25] www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-Rule-Supervision.pdf

suspicious transactions involving multi-layered unhosted wallets that are transactionally distant from TRW.

54. In this context, stablecoin issuers may play a complementary role, as they can be requested by law enforcement authorities (LEAs) to freeze unhosted wallets suspected of containing misused stablecoins. In responding to such requests, issuers may monitor transactions associated with identified unhosted wallet addresses and, where appropriate under the applicable legal framework, submit STR to the FIU.

Limitations of the Blockchain Environment Application to Stablecoins

Cross-Chain activity

55. Blockchain networks and their ecosystem developers increasingly prioritise the development of interoperability for stablecoins compared to other virtual assets. This interoperability allows stablecoins to operate across multiple blockchains and jurisdictions, enabling efficient cross-border transfers.[26] While this fosters legitimate remittances and enhances liquidity, it may also increase opportunities for multi-chain flows to be exploited by threat actors and for transaction trails to be obscured, thereby posing additional challenges for AML/CFT/CPF efforts.

56. Market analysis indicates that sanctioned entities and other threat actors are increasingly using stablecoins, including through cross-chain activities, which may be exploited to fragment transaction flows and complicate traceability as funds move across blockchain networks. This challenge may be further exacerbated where chain-hopping techniques involving multiple blockchains are used, given that individual blockchains operate in isolation and are unable to natively interact with other blockchain networks.[27] Interoperability across multiple blockchains may weaken a key control available to stablecoin issuers, namely the ability to freeze or blacklist assets, where centrally issued stablecoins circulate on other blockchains in the form of newly created (wrapped) stablecoins of the original stablecoins.[28]

Data Gaps

57. The blockchain-based architecture of stablecoins both helps and hinders AML/CFT oversight. Although every transaction is immutably recorded on public blockchains, these records lack critical context and are pseudonymous therefore the collection of CDD information including geographical location, in line with Recommendations 10 and 15 is critical in order to ensure that law enforcement has the ability to obtain information from VASPs and FIs. In addition, the lack of information on the geographical location of underlying wallets may undermine competent authorities' ability to cooperate effectively with relevant foreign counterparts.

58. It is critical to highlight that not all transactions occur on-chain. For example, VA transactions between customers of the same VASP are mostly conducted off-chain, with asset transfers recorded only in the VASP's internal ledger, while relevant customer information, potentially including data related to customer location, is held within the VASP's internal systems. These transfers are usually faster and cheaper because they avoid network fees and block confirmation times, however, when the VASP is unlicensed or unregistered, there is no intermediary collecting customer identification information and filing suspicious transaction reports, complicating the ability of law enforcement to detect and investigate illicit activity.

[26] Considerations for the use of stablecoin arrangements in cross-border payments (BIS, 2023)
[27] https://go.chainalysis.com/2025-Crypto-Crime-Report.html
[28] What Are Wrapped Tokens? A Practical Guide to Cross-Chain Assets

Further, exchanges, issuers, and custodians may pair on- and off-chain data to identify potentially illicit activity, regulators and law enforcement do not have direct access to off-chain data or identified patterns.

Part Two:
Good Practices to Mitigate Misuse of Stablecoins, Including for P2P Transactions

Effective Implementation of FATF Standards

59. It is critical that jurisdictions place AML/CFT obligations on VASPs in the stablecoin ecosystem, including stablecoin issuers and intermediary VASPs . These obligations are detailed in Recommendation 15 of the FATF Standards and should include the implementation of preventive measures in accordance with Recommendations 9-21.[29] Given the number of stakeholders in the stablecoin ecosystem, clear delineation of the specific AML/CFT obligations of each party is important to drive compliance. Jurisdictions should also ensure that relevant AML/CFT obligations apply to financial institutions involved in stablecoin arrangements, including custodians of reserve assets for stablecoin issuers.

Box 5: Japan – Implementation of Measures on Issuers and Intermediaries

Both stablecoin issuers and intermediaries are subject to AML/CFT obligations under the Act on Prevention of Transfer of Criminal Proceeds. Eligible issuers - funds transfer service providers and trust companies- must perform CDD at issuance and redemption and implement risk mitigation measures such a restricting transfers linked to suspected crime, based on information obtained from blockchain analytics firms or investigative authorities. Intermediaries handling domestic or foreign stablecoins in Japan must register as Electronic Payment Instruments Exchange Service Providers and comply with AML/CFT obligations such as CDD, STR, and compliance with Travel Rule. In light of ML risks associated with decentralized exchanges (DEX), consideration is being given to imposing proportionate and appropriate AML/CFT obligations especially on its apps and other user interfaces, subject to further international discussion in this area.

Source: Japan

60. However, the stablecoin ecosystem is complex, and allocating appropriate AML/CFT obligations to the relevant stakeholders is not straightforward. In practice, a relatively small

[29] In resolution 2462 (2019), the UNSC also strongly urged all States to implement the comprehensive international standards embodied in the FATF revised Recommendations. Further guidance is included in the UNSC Counter-Terrorism Committee, "Non-binding guiding principles on preventing, detecting and disrupting the use of new and emerging financial technologies for terrorist purposes", January 2025, S/2025/22.

number of jurisdictions have implemented regulation for stablecoins that explicitly takes into account their characteristics that differ from other virtual assets. (see Box 5).

Box 6. Case studies: – AML/CFT Obligations in the Stablecoin Ecosystem

EU

Stablecoins are classified under the Markets in Crypto-Assets Regulation (MiCA) into E Money Tokens (EMTs), linked to a single fiat currency, and Asset Referenced Tokens (ARTs), which are not e money tokens and purport to maintain a stable value by referencing another value or right or a combination thereof (including one or more official currencies). ART issuers are legal persons established in the EU that have obtained an authorization under Article 16 of MiCA; however, issuing ARTs alone does not make ART issuers AML/CFT obliged entities. Exchange services between ARTs and other crypto assets or fiat currencies, custody of ARTs, and services around issuance (e.g., placing of ARTs, reception and transmission of orders) require a Crypto Asset Service Provider (CASP) authorization, and as obliged entities CASP obligations include risk policies, customer identification and verification, transaction monitoring, suspicious transaction reporting, and sanctions/asset freezing procedures. Competent authorities consider ML/TF risks when granting, refusing, or withdrawing an authorization from an issuer of ARTs typically check AML/CFT related criminal convictions of members of the management body and shareholders with qualified holdings. In addition, the issuer needs to provide information on his arrangements with CASPs (if any), and especially the procedures in place to ensure compliance with the obligations in relation to the prevention of money laundering and terrorist financing under Directive (EU) 2015/849. Competent authorities can refuse to grant authorisation if the applicant issuer's business model might expose the issuer or the sector to serious risks of money laundering and terrorist financing. The absence of any obliged entity intermediary in the offering and placing of ARTs by that issuer may be an indication of such a risk and a competent authority may rely on this provision to refuse authorisation. Thus, although ART issuers are not obliged entities, they must ensure ongoing sound ML/TF risk management. EMTs are issued by authorized credit institutions or electronic money institutions, which are subject to AML/CFT obligations.

Kazakhstan

In the Astana International Financial Centre (AIFC), stablecoin issuers and intermediaries are subject to comprehensive AML/CFT obligations under the AIFC Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Rules (AML Rules). To issue fiat- or commodity-backed stablecoins, an issuer must obtain an Astana Financial Services Authority (AFSA) licence to provide money services in relation to digital assets.

Licensed issuers must implement robust CDD at issuance, redemption and other touchpoints—verifying customers and beneficial owners, conducting enhanced due diligence for higher-risk activity, and monitoring transactions on an ongoing basis. They must also have procedures to identify, restrict or freeze stablecoins

linked to illicit activity, informed by blockchain analytics, law-enforcement information or AFSA directions. Compliance is reinforced by operational requirements: fully backed, segregated reserves; monthly reconciliations; and annual independent audits reported to AFSA and published unless otherwise directed.

Intermediaries facilitating trading, exchange or transfer of stablecoins within the AIFC must be authorised and comply with full AML/CFT obligations, including CDD, record-keeping, suspicious transaction reporting, sanctions screening and the Travel Rule. Issuers and intermediaries must ensure that discontinuation, recovery or wind-down protects holders and does not create vulnerabilities. Together, these measures integrate AML/CFT safeguards with governance, prudential and operational controls to ensure transparent and secure stablecoin activity in the AIFC.

Stablecoin Issuers Applying Controls

61. The FATF Standards require issuers to apply preventive measures, as detailed under Recommendation 15 of the FATF Standards, to stablecoin issuers. These include CDD, record keeping, detection and reporting of suspicious transactions, and compliance with the Travel Rule, among others. Stablecoin issuers should always apply preventive measures to their customers in the primary market (those who purchase or redeem the stablecoin directly from/to the issuer).

62. Jurisdictions may want to consider how existing AML/CFT/CPF obligations could apply in the secondary market and in particular how to leverage the unique technological capabilities of issuers to execute certain smart contract functions, such as a burn or freeze. In particular, issuers can determine the issuance and redemption of their stablecoins at any time. In addition, the issuer can embed freeze and burn functions in the stablecoin's smart contract and exercise them as needed.

63. While they can monitor the status of on-chain circulation and stablecoin balances and transfers at the level of the blockchain addresses, the identities of the stablecoin holders are not publicly available on the blockchain. Where stablecoins are held with a VASP, customer identity information may be available to competent authorities through lawful requests to the relevant VASP, but this information is not readily available to the issuer. Where stablecoins are held in unhosted wallets, only the pseudonymous blockchain address is observable on-chain and no underlying CDD information is available. Notwithstanding the inability to identify the actual holder, where an address is determined to be linked to criminal activity, executing freezing functions remain feasible.

64. Jurisdictions may want to also consider whether, on the basis of risk and context, stablecoin issuers should be required to proactively monitor the location and use of their stablecoins in the secondary market with the support of blockchain analytics tools, and whether they should be subject to proportionate additional measures. Such measures could include regular reporting on the circulation of their stablecoins in secondary market.

65. The smart contract is the core piece of code that controls how the stablecoin works on the blockchain, and it can be programmed to execute specific conditions that must be satisfied before the contract allows an action to happen in both primary and secondary market transactions. Issuers can use the programmability afforded in smart contracts to either allow

only certain wallet addresses to transact in the stablecoin (allow-listing) or to prevent certain wallet addresses from transacting in the stablecoin (deny-listing).

- *Allow-listing or whitelisting*: Stablecoin issuers can control who can hold, receive or transfer a stablecoin by permitting only pre-approved entities or addresses to use it. This is possible by adding an access control list to the stablecoin smart contract; if the wallet address sending/receiving the stablecoin is not on the access control list, the transaction is automatically rejected. CDD requirements, either performed directly by the stablecoin issuer or by an approved third-party provider, can be included as part of the pre-approval process and periodically repeated as necessary to fulfil ongoing due diligence obligations. Allow-listing can mitigate the risk of transactions with unhosted wallets, since it requires the identification of the underlying user before the transaction can be executed.
- *Deny-listing or blacklisting*: Stablecoin issuers can restrict specific wallet addresses or entities from holding, receiving and transferring stablecoins. This is the opposite of allow-listing, where the stablecoin issuer adds a deny control list to the stablecoin smart contract; if the wallet address sending/receiving the stablecoin is on the deny control list, the transaction is automatically rejected. The criteria for adding addresses to the deny control list may be informed by third-party solutions, including blockchain analytics and law enforcement data. Deny-listing can help competent authorities freezing wallet addresses with a stablecoin balance.

Box 7: Switzerland – risk mitigation of unhosted wallets

In Switzerland, a financial institution ("X AG") plans to issue Swiss Franc-denominated stablecoins through its wholly owned subsidiary ("Y AG"). To mitigate risks associated with unhosted wallets, X AG and Y AG will implement an on-chain allow-listing procedure via smart contracts.

Transactions will only be permitted between wallets registered on the allow list, which may include both hosted and unhosted wallets. The allow list will be automatically updated once a new wallet holder meeting the criteria is identified. Unhosted wallet holders will be verified by Swiss banks, VASPs, or foreign banks subject to regulatory standards similar to those in Switzerland.

After successful identification, the unhosted wallet will be added to the allow list, enabling transactions with other verified wallets. Hosted wallets will be identified and allow-listed by the banks or VASPs that manage them.

Source: Switzerland

66. The deny-list approach is used more frequently, but it is more reactive—as issuers typically deny a wallet based on outreach from law enforcement or identification on a national sanctions list. An allow-list is a more proactive approach but may push users who do not want to be identified for privacy reasons out of the stablecoin ecosystem.

Box 8: France – Compliance measures taken by stablecoin issuers

In France, practice shows that stablecoins issuers and virtual asset service providers use blockchain analytics tools in order to trace stablecoins on-chain and identify potentially risky transactions. This monitoring covers both primary market participants (initial holders post-issuance) and subsequent holders on the secondary market. These tools enable issuers to detect transactions involving blockchain addresses flagged as exposed to money laundering or terrorist financing risks. Risk exposure can be assessed either directly (regarding the holders themselves) or indirectly (regarding their counterparties). Furthermore, some stablecoins issuers have embedded various features in the stablecoin's smart contract, such as allow-listing, deny-listing and blocking/freezing capabilities to be activated on request of the public authorities.

67. Stablecoin issuers may also take, or be required to take, other risk mitigation measures such as:

- Transaction limits: Placing limits on the amount per transaction or the total amount transferred per day by wallet addresses or a clearance of pending transactions to mitigate risk in secondary market transactions may also complement a deny-listing or an allow-listing approach in order to reduce the risk of circumvention in case of deny-listing and foster inclusion in case of allow-listing.[30]
- Block, Freeze and Withdraw Capabilities:[31] Stablecoin issuers are encouraged to implement technical measures to be able to block, freeze and withdraw (e.g., by burning and re-issuing) stablecoins at any time if there are (intended) transactions to or from non-allow-listed or deny-listed wallets. This capability can also enable stablecoin issuers to comply with orders from an authority in accordance with applicable law (e.g. confiscation by a law enforcement agency).

[30] Transaction limits are allowed under the FATF framework to mitigate potential financial crime risks linked to accounts that have not been subject to regular KYC/CDD, as indicated in the FATF financial inclusion guidance (paragraph 142) www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Financial-Inclusion%20-Anti-Money-Laundering-Terrorist-Financing-Measures.pdf

[31] Blocking refers to a stablecoin issuer's ability to prevent a specific transaction from being processed without necessarily freezing the holder's entire wallet. This can include stopping transfers to certain addresses, such as sanctioned entities, or rejecting a transaction when conditions like sender or receiver authorization are not met. Freezing, by contrast, refers to the issuer's ability of immobilize a specific wallet address, preventing it from moving its tokens.

Using Advanced Tools for Detecting and Monitoring Suspicious Transactions

Public Sector Use of Tools

68. Blockchain analytics tools can be useful for identifying ML/TF/PF risks in the stablecoin ecosystem, and the FATF has previously analysed and encouraged the use of such tools.[32] Other international organisations, such as the UNSC Counter-Terrorism Committee, have taken a similar approach.[33] Technological advancements, especially in artificial intelligence, machine learning and big data analytics are likely to may have the potential to enhance the capabilities and potential use of these tools for AML/CFT/CPF purposes.

69. Jurisdictions should be mindful of the limitations of blockchain analytics tools, including their challenges reliably detecting sophisticated obfuscation techniques used by threat actors, the heterogeneous capabilities and methodologies of analytics providers, the costs of proprietary licences, and the specialised technical skills required to interpret their outputs. These tools are most effective when deployed in combination with each other and alongside traditional investigative techniques, as well as expert human judgement by personnel trained in virtual asset investigations.

[32] fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf; 2024-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf

[33] UNSC Counter-Terrorism Committee, "Non-binding guiding principles on preventing, detecting and disrupting the use of new and emerging financial technologies for terrorist purposes", January 2025, S/2025/22, para. 22(m).

Box 9. China: Use of blockchain analytical tools to detect unauthorised stablecoin activities

Although China prohibits activities related to virtual assets, including stablecoins, it has formed good practices for risk identification and mitigation through a "regulatory authority-led, multi-party collaboration" model. The core practices include:

1. Application of Technical Tools: On-chain Monitoring and Intelligence Analysis

Virtual asset monitoring platform: The People's Bank of China has established a monitoring platform that has achieved on-chain data analysis and penetration tracking capabilities. It extensively collects data from various public chains, continuously expands the risk tag library, and consolidates the data foundation for monitoring and analysis. The core functions of the monitoring platform include:

- (1) Virtual currency issuance monitoring.
- (2) Virtual currency wallet tag profiling. The tag types cover multiple risk scenarios such as virtual currency exchanges, underground banks, telecommunications fraud, online gambling, illegal fund-raising, online extortion, terrorist financing, proliferation financing, and sanctions lists.
- (3) Wallet relationship network graph. This function analyses the target wallet specified by the user and its transaction counterparty wallets, converts complex blockchain transaction data into an intuitive relationship network, and shows the complete transfer chain of virtual currency funds from the source to the destination.
- (4) Abnormal transaction monitoring and identification. Establish and continuously optimise the monitoring and early warning model for abnormal transactions involving virtual currencies, conduct in-depth mining and risk assessment of on-chain transaction behaviours, and monitor and identify various risky transactions.
- (5) Visual tracking of on-chain transactions. Track the upstream and downstream transaction-related wallets of core wallets through visualization tools.

2. On-chain data connection of financial institutions: Some large banks and third-party payment institutions conduct on-chain analysis and tracking of virtual currencies.

Source: China

Private Sector Use of Tools

70. Some jurisdictions require stablecoin issuers and other entities involved in stablecoin arrangements to use blockchain analytics tools to mitigate illicit finance risks, while others

encourage their use through guidance and other measures. These tools can be but one important tool in the toolkit to prevent the misuse of stablecoins. The FATF recognizes the utility of blockchain analytics and encourages jurisdictions to provide information to stablecoin issuers and other entities involved in stablecoin arrangements on how to best assess and appropriately use blockchain analytics tools to identify and mitigate ML/TF/PF risks at the institutional level.

Box 10: Singapore - private sector use of blockchain analytics tools

DPTSP A is a licensed Major Payment Institution ("MPI") providing cross-border money transfer and digital payment token services. A transactional review conducted by DPTSP A found 2 wallets (wallet 1 and wallet 2) with indirect exposure to a wallet linked to terrorism financing. DPTSP A leveraged on blockchain analytics tools to review high-risk transactions one hop away, which led to the detection of this exposure.

Wallet 1 and wallet 2 held by DPTSP A received USD 5.9m and USD 250k worth of stablecoin USDT from an external wallet (wallet 3) respectively. On-chain analysis showed that wallet 3 had received USD 200k worth of USDT on Tron from a wallet with nexus to terrorism financing. Wallet 3 was also blacklisted by the issuer of the stablecoin from being able to transact USDT to and from this wallet, likely due to having direct nexus to a sanctioned wallet address.

Source: Singapore

Effective Supervision of Stablecoin issuers and other entities involved in stablecoin arrangements

71. The FATF has provided guidance on best practices for VASP supervisors in its report on Best Practices for Travel Rule Supervision.[34] These practices are equally applicable to supervisors overseeing stablecoin issuers and other obliged entities involved in stablecoin arrangements. In addition, supervisors should consider the risks of stablecoins, and the application of risk mitigation measures unique to stablecoins when considering licensing and market entry of entities and products, particularly considering whether mass adoption is considered as a factor in VASPs' risk assessments.[35]

[34] www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-Rule-Supervision.pdf

[35] G20 report paragraph 77 and para 139 of the 2021 Guidance.

Box 11: Hong Kong China Exploring technologies to mitigate anonymity challenges

The Hong Kong Monetary Authority (HKMA) introduced a regulatory regime for stablecoin issuers under the Stablecoins Ordinance. The HKMA has published regulatory guidelines setting out the AML/CFT requirements applicable to stablecoin issuers.[36]

As the inherent ML/TF risks can vary substantially between different types of stablecoin arrangement, the HKMA has adopted a risk-based but cautious approach when formulating the AML/CFT requirements. As part of the licensing process, applicants are required to assess the ML/TF risks associated with their stablecoin arrangement, including any risks associated with secondary markets and unhosted wallets, and apply proportionate mitigating measures. While applicants may adopt an "allow-listing" approach at the initial stage of their stablecoin issuance business, they are also expected to submit planned mitigating measures over the medium-to-long term, to address any increased risks where the business grows, or they plan to operate in a more open-ended environment. During private sector engagements undertaken as part of the exercise, several evolving technology solutions (e.g. decentralised digital identity[1]) and blockchain protocols (e.g. ERC3643) aimed at mitigating anonymity challenges arising from circulation of stablecoins in the secondary market have been considered. The HKMA is closely monitoring these technological developments to ensure that its stablecoin regulatory regime reflects local circumstances while aligning with international standards and practices.

Source: Hong Kong, China

[1] See FATF Guidance on Digital Identity

72. Supervisors should develop and maintain the technical knowledge to understand and guide the implementation of regulation in stablecoin arrangements. They should not only perform a check the box test (e.g., "Does a stablecoin issuer have a blockchain analytic tool in place?") but must be able to assess themselves whether the implemented tools and controls are effective in mitigating ML/TF/PF risks. On this basis, supervisors should also provide guidance and lead engagement with the private sector to learn about emerging risks and determine the most effective supervisory practices in the stablecoin ecosystem.

73. Some jurisdictions have taken a proactive approach by requiring or encouraging cooperation among supervisors [37] of stablecoin arrangements. Emerging good practices include the establishment of supervisory colleges - cooperative frameworks that bring together home and host supervisors to share information and coordinate supervision on entities operating in multiple countries. The Financial Stability Board (FSB) has noted that global stablecoin issuers may exhibit characteristics similar to other international financial

[36] www.hkma.gov.hk/eng/key-functions/international-financial-centre/stablecoin-issuers/

[37] On supervisory cooperation, FATF noted international co-operation between supervisors; see FATF (2021) Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers, page 103, paragraphs 357

institutions and that supervisory colleges can help address cross-border oversight challenges when properly supported by information-sharing arrangements. Under such frameworks, jurisdictions may also consider permitting unregulated stablecoin issuers to voluntarily submit a single license application to obtain authorisations covering activities across multiple jurisdictions.

Box 12: Use of Supervisory Colleges for Stablecoin Oversight in the EU

Under MiCAR, the supervisory college framework applies only in specific circumstances and is focused on a narrow set of activities—namely, the supervision of issuers issuance of significant asset-referenced tokens (ARTs) and significant electronic money tokens (EMTs). An issuer of an ART or an EMT is deemed to be significant when certain quantitative and qualitative conditions are met, for example in terms of number of holders, value of the token issued, value of transactions per day, and interconnectedness with the financial system.

In such cases, the EBA must establish and chair supervisory consultative colleges to coordinate supervisory activities related to the supervision of issuers of significant ARTs and EMTs issuance. Since issuers of significant asset-referenced tokens and of significant e-money tokens are usually at the centre of a network of entities that ensure the issuance, transfer and distribution of such crypto-assets, the members of the college of supervisors for each issuer should therefore include, amongst others, the competent authorities of the most relevant trading platforms for crypto-assets, in cases where the significant asset-referenced tokens or the significant e-money tokens are admitted to trading, and the competent authorities of the most relevant entities and crypto-asset service providers ensuring the custody and administration of the significant asset-referenced tokens and of significant e-money tokens on behalf of holders. The college of supervisors for issuers of significant asset-referenced tokens and of significant e-money tokens should facilitate the cooperation and exchange of information among its members and should issue non-binding opinions on, amongst others, changes to the authorisation of, or supervisory measures concerning, such issuers.

Source: European Union

Robust Public-Private Sector Collaboration

74. Collaboration between the public and private sector is essential in the virtual asset space, where risks are evolving rapidly and timely responses to ML/TF/PF is crucial to recover assets. The FATF sees value in the public sector working with stablecoin issuers and other entities involved in stablecoin ecosystem to work together to enhance understanding of evolving trends, strengthen co-operation on typologies and risk indicators, and build the knowledge and skills of relevant experts, thereby reinforcing the integrity and security of the stablecoin ecosystem.

Following Investigative Leads

75. When stablecoins are misused through AML/CFT obliged entities, competent authorities may seek information through both cooperative and coercive means. The investigative process is more difficult when transactions are conducted through unhosted wallets as the is no entity with whom to cooperate or coerce. Investigators should do have some tools available to pursue illicit transactions involving unhosted wallets:

- Tracing transaction flows to exit-points (cash-out or off-ramps): Identification of potential cash-out or off-ramps by using commercial or open source blockchain analysis tools to trace funds from target address through intermediary addresses and protocols to potential exit points
- Set-up alerts in relation to the address to assess activity and behaviour
- Conduct open-source intelligence to increase the attribution strength
- Integration of on-chain data with physical-world investigative methods

76. For certain centralised stablecoins like USDT or USDC, the stablecoin issuer may be contacted directly as they have the technical ability to freeze the stablecoins via smart contract functions.

ML/TF/PF Risks Mitigation measures for Unhosted Wallets and P2P Transactions

77. The FATF Standards are built on a foundation of the risk-based approach. While the FATF Standards do not explicitly apply to unhosted wallets and P2P transactions, jurisdiction should consider their ML/TF/PF risks, including for P2P transactions, and mitigate those risks. The FATF, notwithstanding the challenges for jurisdictions to obtain reliable and complete data on the unregulated market, advises jurisdictions to seek to understand to the greatest extent possible the frequency of P2P transactions in their jurisdiction and associated ML/TF/PF risks. Jurisdictions should also seek to implement appropriate risk mitigation measures in light of the estimated size and risk level of P2P transactions.[38]

78. Across the Global Network, jurisdictions and the private sector have taken various approaches to mitigate risks including:

a. VASPs limiting the amount of funds that can be transferred by their customers to unhosted wallets

b. VASPs applying enhanced CDD measures for transactions with unhosted wallets, including verification of the unhosted wallet's beneficial owner identity.

c. VASPs using blockchain analytics tools to determine the risk-level of their customers' counterparties who own unhosted wallets.

d. Entities involved in stablecoin arrangements subjecting unhosted wallets to AML/CFT obligations including CDD at time of issuance and redemption.

e. Prohibiting or denying licenses to platforms that allow transfers to unhosted wallets.

[38] FATF(2024) Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers, page 5, paragraphs 37-41, 105-107

Box 13. Singapore – AML/CFT obligations for Unhosted Wallets

For transactions involving unhosted wallets, Digital Payment Token Services Providers (VASPs in Singapore) are expected to put in place enhanced risk mitigating measures, given the specific ML/TF risks associated with such transfers. Other examples of risk mitigating measures that VASPs are expected to implement include limiting VA transfers to only first party transfers and verifying ownership of customer's unhosted wallet, identifying beneficiary, enhanced monitoring of customer account, and understanding purpose of transaction.

Source: Singapore

Box 14. Germany: mitigation of risks associated with redemptions to unhosted wallets

An entity applied for a licence to issue euro-denominated e-money tokens, which may be redeemed upon request. The funds received in exchange for tokens will be invested, while clients—exclusively businesses—will distribute these tokens to end customers.

The entity was granted permission under the following conditions: Investment of reserves entails liquidity and concentration risks. To mitigate these, reserves will be diversified and restricted to short-term, highly liquid instruments. Business clients are not considered to present elevated AML/CFT risks. However, as the entity has no visibility over the ultimate beneficiaries, business clients will be subject to enhanced due diligence.

Given the risks associated with redemptions to unhosted wallets, particularly the potential for misuse in illicit activities, the following safeguards will be implemented:

- **Identity Verification:** The Entity must verify the identity of the wallet owner before processing any redemption to a self-hosted wallet.
- **Blockchain Forensics:** The Entity will deploy tools to trace the origin and destination of virtual assets, with particular attention to high-risk or sanctioned addresses.
- **Transaction Limits**: Client-specific transaction thresholds will be applied to detect and prevent suspicious activity, with lower limits for higher-risk clients or jurisdictions.
- **IT Monitoring**: The system must include ongoing surveillance against whitelists and blacklists, including integration with EU and international sanctions lists.

Source: Germany

Conclusion

79. Stablecoins have seen a rapid rise in adoption due to the characteristics of the stablecoins themselves, and the confidence given to users of their inclusion in regulatory regimes. As they have grown more popular, they have also been used more frequently for ML, TF and PF, and reporting indicates that they are the most popular virtual asset for illicit transactions. The FATF has addressed stablecoins as either virtual assets or traditional financial assets, depending on their structure, and has required jurisdictions to apply the same AML/CFT/CPF obligations to intermediaries involved in stablecoin arrangements, including VASPs and financial institutions.

80. Notwithstanding the FATF's framework, stablecoins are exposed to heightened ML/TF/PF risks when transferred on a P2P basis via unhosted wallets. These vulnerabilities are exacerbated by their characteristics such as the price stability and ample liquidity, which can make stablecoins more likely to be used in P2P transactions. Available analysis indicates that a significant proportion of illicit stablecoin transactions occurs via unhosted wallets including P2P, which allows actors conducting these transactions to circumvent AML/CFT obligations. Cases indicate that threat actors have used stablecoins to purchase prohibited goods without cashing out through intermediaries, however, data remains limited regarding the broader use of stablecoins for the purchase of goods and services or for P2P transactions. Therefore, it is important for jurisdictions and relevant stakeholders to continue to closely monitor whether stablecoins are increasingly used for purchases without reliance on traditional on- and off-ramps, and the extent to which accurate data on the scale and proportion of P2P transactions can be obtained.

81. The report identifies a range of good practices that could be implemented by jurisdictions and the private sector to mitigate these risks and makes recommendations for implementation. These include tailored regulatory frameworks for stablecoin issuers, enhanced risk mitigation measures for unhosted wallet transactions, the use of advanced blockchain analytics, programmable controls embedded in smart contracts and strengthened domestic and international co-operation mechanisms.

Recommended Actions

For Jurisdictions

I. Jurisdictions should apply R.15 to entities involved in stablecoin arrangements, ensuring that stablecoin issuers, intermediary VASPs, and other relevant participants are subject to clear, enforceable AML/CFT obligations. Jurisdictions should define the roles and responsibilities of all participants throughout the stablecoin ecosystem and impose appropriate AML/CFT obligations using a risk-based approach.

II. Jurisdictions should consider effective AML/CFT measures specific to stablecoin issuers and other obliged entities, such as requiring issuers to maintain and execute the technical capability to burn, freeze, and withdraw in the secondary market, apply CDD at the redemption stage, or limit issuance on high-risk chains. Jurisdictions should also consider requiring stablecoin issuers to implement allow-lists and deny-lists as appropriate, using a risk-based approach. Jurisdictions should institutionalise rigorous pre-launch and pre-licensing supervision and compliance reviews to mitigate stablecoin ML/TF risks before launch.

III. Jurisdictions should prioritise the development of robust technical capabilities by competent authorities, including supervisors and LEAs. This includes building technical expertise to understand evolving risks, typologies, business models, smart contract functionalities, and cross-chain transaction mechanics and to strengthen capabilities to effectively utilize blockchain analysis tools.

IV. Jurisdictions should consider establishing multinational supervisory colleges to supervise stablecoin issuers and other entities involved in cross-border stablecoin arrangements, when necessary.

V. Jurisdictions should provide competent authorities, especially supervisors and LEAs, with the necessary tools to cooperate swiftly with domestic and international counterparts, including through established channels, MOUs, and legal provisions that enable the prompt exchange of information on stablecoin arrangements.

VI. Jurisdictions should actively monitor existing macro vulnerabilities and loopholes in the stablecoin ecosystem, including the volume and risk posed by P2P transactions via unhosted wallets and the use of informal or unlicensed/unregistered redemption channels. Supervisors should understand and assess the ML/TF/PF risks presented by business models allowing the use of stablecoins for payment and investment purposes and apply proportionate mitigating measures.

VII. Jurisdictions should consider whether stablecoin issuers, on the basis of risk and context, should be required to proactively monitor the location and use of their stablecoins in the secondary market with the support of blockchain analytics tools, and whether they should be subject to proportionate additional reporting requirements.

VIII. Jurisdictions should consider establishing structured public-private partnerships to strengthen cooperation between competent authorities and stakeholders in the stablecoin ecosystem on typologies, risk indicators, and emerging threats. They should also consider creating tactical partnerships, particularly when investigations involve off-chain transactions or the freezing or burning of stablecoins.

IX. Jurisdictions should consider establishing sandboxes with industry participants, where appropriate, to develop standards and solutions that enable innovation while safeguarding against misuse, such as through smart contract monitoring, blockchain forensics, or automated sanctions screening.

For the Private Sector

I. VASPs and FIs should ensure that they understand the different types of stablecoin arrangements and the ML/TF/PF risks at the issuance, circulation and redemption stages. VASPs and FIs should apply adequate and robust AML/CFT/CPF measures to all entities involved in stablecoin arrangements and transactions.

II. Stablecoin issuers should be required to assess and mitigate ML/TF/PF risks associated with their customers. They are also strongly encouraged to take measures to mitigate risks in the secondary market, including monitoring stablecoin usage and implementing specific governance arrangements and technical measures embedded in stablecoin design.

III. Stablecoin issuers are encouraged to implement technical measures that enable them to block, freeze and withdraw (for example, by burning and re-issuing) stablecoins at any time and to program smart contract to include AML/CFT/CPF control measures, such as CDD requirements.

IV. Stablecoin issuers should consider making public a centralised contact for law enforcement that is monitored 24/7, and able to take measures to expeditiously freeze stablecoins.

Annex A: List of Risk Indicators

Unusual Transaction-related Indicators

1. Rapid cross-border movements of stablecoins inconsistent with customer profile.
2. Transfer of large value of stablecoins, especially if obtained from the recent conversion of other VAs to multiple beneficiaries who do not appear to have any connection with the person concerned and are carried out within a limited time frame.
3. Requests for the transfer of stablecoins from different and apparently unrelated parties to the same counterparty address; or crediting of significant amounts of stablecoins from multiple senders who appear to have no connection with the person concerned, especially over a limited time frame.
4. Use of an account opened with the VASP as a transit account for overall large-countervalue transfers of VAs to and from other persons.
5. Large-value transactions in stablecoins by the same person in a short period of time, in cash or by using multiple devices (e.g., ATMs) or IP addresses, especially if they are apparently located in geographically locations distant from each other or from the location in which the person concerned lives or operates, or of using IP addresses different from those typically used by the person concerned.
6. Stablecoins are used to fund gambling balances or to create false 'refunds' where purchases are reversed to wallets not linked to the original payer, masking ownership and integrating illicit value into ostensibly legitimate merchant flows.
7. Rapid conversions between fiat currencies and stablecoins with no evident economic rationale.
8. Rapid exchange of stablecoins for other stablecoins or VAs with no evident economic rationale.
9. Recurrent transactions in VAs that appear to be linked to peer-to-peer exchange mechanisms, for amounts corresponding to an overall significant value in legal tender.
10. Conversion of stablecoins into legal tender for an overall relevant countervalue where the virtual assets have been deposited recently, including through several fractional transactions.
11. Multiple accounts or payment instruments used by the same person to carry out conversion transactions from/to stablecoins, especially within a limited timeframe and for an overall significant countervalue.

12. Requesting the conversion of stablecoins into legal tender under disadvantageous economic conditions, including the payment of higher fees than those generally charged in the industry.
13. Multiple transactions involving the conversion of stablecoins into one or more VAs and the simultaneous transfer of such assets, even by means of transactions involving small unit amounts, until the relevant balance reaches zero, especially if the funds for the purchase of the stablecoins were generated through transfers of legal tender from different accounts.
14. Recurrent purchase and sale of stablecoins in cash through transactions which, due to their characteristics (e.g. amount, date, credit/debit address of the stablecoins), appear to be artificially split in order to circumvent the statutory threshold for the transfer of cash between different persons or other internal limits on use predetermined by the obliged entity.
15. Recurrent large-value transactions in legal tender or stablecoins, that are preceded or followed by a long period of time in which no transactions are carried out.
16. Multiple large-value transactions in stablecoins, in favour of newly opened or previously inactive accounts.
17. Purchase of stablecoins issued under a multi-jurisdictional scheme – in one jurisdiction and filing redemption request with a co-issuer in another jurisdiction without any valid economic rationale.

Anonymity-related Indicators

1. Stablecoin transfers involving unhosted wallets that are multiple hops away from Travel Rule-covered wallets (TRW).
2. The unhosted wallet is suddenly activated after a long period of inactivity, completes multiple cross-chain transactions in a short period of time, and then becomes inactive again.
3. Unhosted wallets frequently conduct "large-value two-way transfers" with hosted wallets of offshore stablecoin exchanges without reasonable business explanations.
4. The unhosted wallet has transferred funds to addresses of illegal domestic and offshore stablecoin trading platforms and dark web markets or has received funds from these platforms.
5. Use of offshore issuers not authorised or registered in the jurisdiction.
6. Integration with DeFi for swapping stablecoins, liquidity pooling, and yield farming to obscure transaction trails.
7. Smurfed stablecoin transfers are coordinated from overlapping devices, Internet Protocol Autonomous System Numbers (IP ASNs), and browsers, with perennial near instant conversions from fiat to stablecoins via a DEX and off-ramped back into fiat which is executed within sub-hour windows to minimise detection opportunities.
8. Movement of funds between different blockchains using stablecoins to complicate tracing and exploit gaps in blockchain analytics tools.
9. Conducting stablecoin cross-chain transfers across multiple blockchains in a short period of time, with a high cumulative transaction amount.
10. Progressively bridging stablecoins across chains (e.g., TRON to Ethereum and to Solana) and wrap/unwrap stablecoins prior to off ramp, inserting additional contracts and router hops that degrade traceability.
11. Stablecoins combined with mixers, anonymity enhanced coins or privacy wallets to enhance anonymity during the layering stages.
12. Transactions in VAs originating from or directed towards persons/addresses or settled by means of instruments or accounts that appear to be linked, directly or indirectly, to the deep web or in any case to other risky contexts (e.g. mixing, tumbling, unauthorised gambling operators).
13. Proceeds are funnelled through brokered P2P markets and informal OTC desks that accept cash, gift cards, or third-party bank transfers, converting to stablecoins that are layered across multiple wallets before reconverting on an exchange account.

14. Facilitators employ over-the-counter brokers to convert fiat into stablecoins, thereby bypassing exchange-level CDD checks.
15. Use of proxy or anonymisation services (e.g. The Onion Router) capable of hindering the identification of the origin of the internet connection.

TF and PF-related Indicators

1. Numerous donations (often USD 100–15,000 equivalents) to frequently changing wallets that nonetheless exhibit shared artifacts (QR codes, domains, or change addresses), with funds then routed through DEX routers and bridges before reconverging for cash out.
2. Stablecoin inflows labelled as humanitarian support are rapidly diverted, often within hours, into trading activities, mixers, or cross-chain movements, indicating potential operational financing that is masked by cause-based narratives and distributed online fundraising efforts.
3. Dense chains of more than 25 rapid hops, liquidity slicing via DEX aggregators, and pre-off-ramp swaps into anonymity enhancing assets, followed by re-aggregation into procurement wallets associated with brokers and trading companies.
4. Stablecoin payments are directed to intermediaries near free trade zones or logistics hubs, purchasing lab equipment, machine tools, RF components, Unmanned Aerial Vehicle parts, and other dual-use items; invoices and shipment data are often mis-declared while value transfer occurs entirely in stablecoins outside traditional banking channels.
5. Use of cross-chain bridges to traverse analytics and policy gaps between networks and service providers, accessing global liquidity and off-ramping through non-compliant venues that lack effective screening.
6. Off-ramping stablecoins into fiat currency in jurisdictions with weak AML/CFT controls or through non-compliant VASPs.
7. Interaction with high-risk exchanges or sanctioned addresses.
8. Transactions in stablecoins, especially if involving large amounts, engaging addresses for which the information available does not allow to obtain reasonable assurance of the beneficial owner or which are linked, even indirectly, to contexts at risk or to high-risk, non-cooperative or low-tax jurisdictions or to jurisdictions with deficient or inadequate anti-money laundering legislation, in particular with regard to VAs.