39-43 Barbados Avenue | Kingston 5, Jamaica W.I.
Telephone: (876) 906-3010 | www.fscjamaica.org

PROPOSED AML/CFT/CPF GUIDELINES

For Virtual Asset Service Providers

Contents

List of Acronyms 4
1. Introduction 5
2. Scope of Application 5
3. Factors That Give Rise to ML/TF/PF Risk 6
   3.1 Privacy and Anonymity 6
   3.2 Decentralised Business Models 6
   3.3 Cross-Border Nature 6
   3.4 Segmentation 6
   3.5 Acceptability, Immutability, and Convertibility 6
   3.6 Operational Structure 7
4. Risk Management 7
   4.1 Risk Assessment 7
   4.2 Customer Risk 7
   4.3 Product Risk 7
   4.4 Transaction Risk 7
   4.5 Geographical Risk 8
   4.6 Delivery Channel Risk 8
   4.7 AML/CFT Internal Controls 8
5. Customer Due Diligence 8
   5.1 Enhanced Due Diligence 8
   5.2 Blockchain Analysis 9
   5.3 Source of Funds 9
   5.4 Ongoing Monitoring 9
6. Record Keeping 9
7. Implementation of Targeted Financial Sanctions 9
8. Identification and Reporting of Suspicious Transactions 10
   8.1 Indicators of Suspicious Activity 10
      Transaction-Related 10
      Anonymity-Related 10
      Customer-Related 11
      Geographical 11
   8.2 Actions on Detection 11
9. Virtual Asset Transfers — Travel Rule 11
   9.1 Originating VASP Obligations 11
   9.2 Beneficiary VASP Obligations 12

9.3 Intermediary VASP Obligations 12
9.4 Unhosted Wallets 12
9.5 Record Retention 12
9.6 General Compliance.....12

List of Acronyms

Acronym	Meaning
AEC	Anonymity-Enhanced Currency
AML/CFT/CPF	Anti-Money Laundering / Countering the Financing of Terrorism / Counter-Proliferation Financing
CDD	Customer Due Diligence
DeFi	Decentralised Finance
DLT	Distributed Ledger Technology
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FID	Financial Investigations Division
FSC / Commission	Financial Services Commission
goAML	UNODC financial intelligence reporting platform used in Jamaica
IP	Internet Protocol
KYC	Know Your Customer
ML	Money Laundering
P2P	Peer-to-Peer
PF	Proliferation Financing
POCA	Proceeds of Crime Act
POC-MLPRs	Proceeds of Crime (Money Laundering Prevention) Regulations
SAR	Suspicious Activity Report
TF	Terrorist Financing
TPA	Terrorism Prevention Act
UNSCRIA	United Nations Security Council Resolutions Implementation Act
VA	Virtual Asset
VASP	Virtual Asset Service Provider
VASP Act	Virtual Asset Service Providers Act (proposed)

1. Introduction

1. These Guidelines are issued by the Financial Services Commission (the "Commission" or "FSC") to assist Virtual Asset Service Providers ("VASPs"), as defined in the proposed Virtual Asset Service Providers Act ("VASP Act"), in understanding and fully implementing their obligations with respect to anti-money laundering, countering the financing of terrorism, and counter-proliferation financing (AML/CFT/CPF) matters.
2. The FSC is the designated competent authority responsible for regulating and supervising VASPs under the VASP Act, and is designated as the AML/CFT supervisor of VASPs under the Proceeds of Crime Act.
3. These Guidelines are supplementary to the FSC Guidelines on the Prevention of Money Laundering and Countering the Financing of Terrorism and Proliferation (the "FSC AML/CFT/CPF Guidelines") and must be read in conjunction with them. All obligations in the FSC AML/CFT/CPF Guidelines apply to VASPs in full, including requirements on risk assessment frameworks (Section IV), customer due diligence (Section V), the Nominated Officer regime (Section VI), compliance monitoring (Section VII), transaction monitoring and reporting (Section VIII), recordkeeping (Section IX), and Board responsibility and staff integrity (Section X). Where these Guidelines address a matter also covered in the FSC AML/CFT/CPF Guidelines, the provisions of these Guidelines apply in addition to, and not in substitution for, those general requirements.
4. The terms "virtual asset", "virtual asset services", and "virtual asset service provider" carry the meanings given in the VASP Act.

2. Scope of Application

5. These Guidelines apply to all VASPs providing virtual asset services as defined in the VASP Act and applicable legislation — regardless of the technology or method of delivery used, and whether the VASP operates via a decentralised or centralised platform, smart contract, or other mechanism.
6. Each VASP is responsible for maintaining systems, policies, procedures, and staff training to prevent ML/TF/PF, including identification and verification procedures, ongoing monitoring, and record-keeping.
7. These Guidelines apply to the following categories of VASP:
    - virtual asset trading platform operators (or exchanges);
    - virtual asset wallet services providers;
    - virtual asset broker-dealers;
    - virtual asset advisors;
    - virtual asset custodians; and
    - virtual asset conversion service providers.
8. These Guidelines do not apply to persons solely developing or selling virtual asset software or platforms, provided they do not also engage as a business in virtual asset services on behalf of others. A DeFi application as a software programme is not itself a VASP, but any person who maintains control or sufficient influence over DeFi arrangements may fall within the VASP definition where they are providing or actively facilitating VASP services. Hardware wallet manufacturers and other ancillary service providers are similarly excluded to the extent they do not engage in virtual asset activities on behalf of customers.

3. Factors That Give Rise to ML/TF/PF Risk

9. Virtual assets may carry a heightened ML/TF/PF risk by virtue of their characteristics. VASPs should be aware of the following risk factors specific to the virtual asset environment.

3.1 Privacy and Anonymity

10. Privacy-enhancing features and services can obfuscate transactions and inhibit effective CDD. Examples of such features include:
    - mixers or tumblers;
    - anonymity-enhanced currencies (AECs);
    - obfuscated ledger technology;
    - IP anonymisers;
    - ring signatures and ring confidential transactions;
    - stealth addresses;
    - atomic swaps;
    - non-interactive zero-knowledge proofs; and
    - privacy coins.

11. Virtual assets also enable rapid, non-face-to-face cross-border transfers. VASPs should apply risk-based scrutiny to customers and transactions commensurate with their business type and transaction volumes, and should consider deploying blockchain analysis tools to identify connections to high-risk sources including the darknet and blacklisted addresses.

3.2 Decentralised Business Models

12. Where a VASP operates on a decentralised basis, there may be no central server or service provider with overall responsibility for identifying users, monitoring transactions, or acting as a law enforcement contact point. Risk-based mitigation measures — including blockchain analysis — should be applied where VASPs deal with funds originating from decentralised systems.

3.3 Cross-Border Nature

13. VASP connections to multiple jurisdictions give rise to ML/TF/PF risks. VASPs must ensure effective application of all AML/CFT/CPF processes in each jurisdiction in which they operate and must take appropriate steps to compensate for additional risk introduced by cross-border transactions.

3.4 Segmentation

14. Virtual asset infrastructure may involve several entities across different jurisdictions, increasing the risk of partial oversight and hindering law enforcement access. VASPs should collaborate with other value chain participants to maintain a robust AML/CFT/CPF framework and must note that they retain full responsibility for the compliance of any outsourced providers or agents.

3.5 Acceptability, Immutability, and Convertibility

15. The wide availability of virtual asset acceptance points and the ease of exchanging virtual assets for other assets or fiat currency makes transactions harder to track. Once validated on a distributed

ledger, transaction records cannot easily be altered, making recovery of misappropriated assets difficult. VASPs should ensure clients are made aware of these risks.

3.6 Operational Structure

16. VASPs must consider their operational structure in assessing and mitigating risk, including: whether they operate online or in person; the nature and scope of their products and services; the nature of their payment channels; and any product parameters that limit exposure to risk, such as transaction or balance limits.

17. Higher-risk operational indicators include: customers operating multiple accounts or accounts on behalf of third parties; involvement in virtual asset mining in high-risk jurisdictions; use of VPN, Tor, or anonymous email services; requests to exchange into cash, privacy coins, or anonymous electronic money; transactions to newly created addresses; persistent structuring below thresholds; and virtual assets connected to the darknet, ransomware, hacking, fraud, Ponzi schemes, or sanctioned addresses.

18. Lower-risk indicators include: small-value accounts serving financially-excluded customers; product parameters limiting transaction volumes or balances; exchanges sourced from or destined for the customer's own low-risk bank account or whitelisted wallet; low-value payments for goods and services; and blockchain analysis indicating lower risk.

4. Risk Management

4.1 Risk Assessment

19. Prior to engaging in virtual asset service activities, VASPs must carry out a comprehensive and documented risk assessment in accordance with Section IV of the FSC AML/CFT/CPF Guidelines and Regulations 8 and 9 of the AMLRs. This assessment must cover ML/TF risks in relation to customers, countries, geographic regions, products, services, transactions, and delivery channels, and must be repeated for any new products, business practices, delivery mechanisms, or technologies prior to launch. The risk assessment must be documented, kept current, and be readily available to the Commission for examination.

4.2 Customer Risk

20. Customer risk profiles must be periodically updated and used to determine the appropriate level of CDD and ongoing monitoring. VASPs should screen customer and counterparty wallet addresses against available blacklisted and sanctioned address databases and take appropriate action — including restricting or terminating the business relationship — where a positive match is identified.

4.3 Product Risk

21. The features of services offered and virtual assets held, stored, transferred, or exchanged determine overall product risk. Changes to services or virtual assets offered must be assessed for risk impact prior to introduction.

4.4 Transaction Risk

22. Transaction risk should be assessed through blockchain analysis — investigating the provenance of virtual assets, the time elapsed since any higher-risk event, and the proportion of higher-risk

assets within the transaction. Blockchain analysis may be outsourced; however, the VASP retains full regulatory responsibility and must conduct due diligence on any outsourced provider.

4.5 Geographical Risk

23. Geographical risk relates to both the customer's place of establishment and the provenance of the virtual asset. VASPs should take into account publicly available information about the regulatory treatment and use of virtual assets in relevant jurisdictions.

4.6 Delivery Channel Risk

24. VASPs must assess risks related to how customers access their products or platforms, including whether access is online or physical and the manner in which virtual asset accounts are funded.

4.7 AML/CFT Internal Controls

25. VASPs must implement board-approved policies, controls, and procedures to manage and mitigate identified ML/TF/PF risks. Internal controls must be adequate across all operations, departments, branches, and subsidiaries, domestically and internationally. They must include: clear AML/CFT governance with an appointed Nominated Officer at management level; controls to monitor staff integrity; ongoing staff training; and an independent audit function.

26. Operational control measures may include transaction limits; time delays before certain transactions can be carried out; and prohibitions on transfers to third parties where source and destination names do not match. Controls must address all requirements set out in Regulation 6 of the POC-MLPRs.

5. Customer Due Diligence

27. VASPs must apply the full set of CDD measures required in Section V of the FSC AML/CFT/CPF Guidelines, including identification and verification of customers and beneficial owners, obtaining information on the purpose and nature of the business relationship, and conducting ongoing CDD throughout the life of the relationship.

28. For virtual asset exchanges, the customer is generally the person requesting the exchange. For virtual asset wallet service providers, the customer is generally the person on whose behalf the virtual asset is held or transferred.

29. VASPs must apply CDD measures when: establishing business relationships; suspicions of ML/TF/PF arise regardless of exemptions or thresholds; and when doubts arise about the adequacy of previously obtained identification data. For one-off transactions, CDD must be applied to each transaction.

30. Information to be collected may include IP addresses with timestamps, geo-location data, device identifiers, wallet addresses, and transaction hashes. VASPs should match customer and counterparty wallet addresses against available blacklisted address lists and seek to determine the provenance of virtual assets.

5.1 Enhanced Due Diligence

31. Where ML/TF risk is higher — including in circumstances listed in Regulation 7A(2) of the POC-MLPRs — EDD must be applied. Higher-risk indicators include transactions involving high-crime or

high-corruption jurisdictions, pseudonymous or anonymous arrangements, non-face-to-face relationships, and payments from unknown or unassociated third parties.

32. EDD measures may include: corroborating identity against third-party databases; tracing IP addresses; additional information gathering on the customer and nature of the relationship; source of funds verification; and enhanced ongoing monitoring.

5.2 Blockchain Analysis

33. Blockchain analysis is additional to — not a substitute for — standard CDD. It should be applied in line with a risk-based approach having regard to the VASP's business type. Where outsourced, the VASP retains full AML/CFT responsibility and must conduct due diligence on the provider, assessing the quality and coverage of its tools and any limitations in handling anonymity-enhancing mechanisms.

5.3 Source of Funds

34. Evidence of source of funds must be collected for all higher-risk transactions, including: exchanges of virtual assets for fiat or vice versa; exchanges of one virtual asset for another where the customer claims the asset was obtained through mining; and transfers of virtual assets between exchanges. It is good practice to also collect destination-of-funds information. Where a recipient's name has been collected, sanctions obligations apply.

5.4 Ongoing Monitoring

35. VASPs must implement effective risk-based transaction monitoring procedures to detect the origin and destination of virtual assets transferred to or from customers, with particular attention to transfers involving high-risk counterparties or unhosted wallets. VASPs must: track transaction histories to identify sources and destinations; screen wallet addresses against databases of illicit or suspicious addresses; and deploy appropriate blockchain analytics solutions. Where an external solution is used, the VASP retains full compliance responsibility.

6. Record Keeping

36. VASPs must maintain records on transactions and CDD information in line with Regulation 14 of the POC-MLPRs, including: identifying information on all parties; public keys or equivalent identifiers; addresses or accounts involved; the nature and date of the transaction; and the amount transferred. Reliance solely on blockchain data is not sufficient — additional information is required to link wallet addresses to identified persons. All records must be retained for a minimum of seven (7) years and must be readily accessible to the Commission on request.

7. Implementation of Targeted Financial Sanctions

37. VASPs must freeze without delay the assets — including virtual assets — of designated persons or entities, and must ensure no assets are made available to or for the benefit of such persons or entities. Some sanctions lists now include wallet addresses in addition to personal or entity names.

38. Given the speed and finality of virtual asset transactions, sanctions screening must operate in real time or as close to real time as technically feasible prior to executing any transfer. Screening must

cover both customer identities and wallet addresses against the UN Security Council consolidated list and other applicable sanctions lists, and must occur at minimum:

- during customer onboarding;
- at regular intervals — preferably every two weeks, but no less than monthly;
- without delay upon receipt of new or amended listings; and
- prior to executing each transfer of virtual assets.

39. VASPs must deploy blockchain analytics tools to identify wallet addresses linked — directly or indirectly — to designated persons or entities, including through chain-hopping, mixing, or layered transfers. Where assets belonging to a designated person or entity are identified, VASPs must freeze them immediately and report to the Financial Investigations Division (FID) via the goAML portal in accordance with Section V(C) of the FSC AML/CFT/CPF Guidelines and the UNSCRIA.

8. Identification and Reporting of Suspicious Transactions

40. VASPs must have systems capable of flagging unusual or suspicious movements of funds, value, or transactions for further analysis — regardless of whether transactions are fiat-to-fiat, virtual-to-virtual, fiat-to-virtual, or virtual-to-fiat in nature. Suspicions of ML/TF must be reported promptly to the FID via the goAML portal.

8.1 Indicators of Suspicious Activity

41. The following are non-exhaustive indicators of suspicious activity, to be considered in the context of the customer's overall profile and alongside a reasonable assessment of whether a logical business explanation exists.

Transaction-Related

- Structuring of virtual asset transactions in amounts below applicable record-keeping or reporting thresholds; or multiple high-value transactions in a staggered, regular pattern — particularly common in ransomware-related cases — or to newly created or previously inactive accounts.
- Immediate transfer of virtual assets to multiple VASPs, especially those in jurisdictions with weak or absent AML/CFT regulation.
- Receipt or deposit of virtual assets from addresses identified as holding stolen funds or linked to theft.
- Deposit of virtual assets followed by immediate withdrawal to a private wallet, effectively using the VASP as a mixer.
- Conversion of large amounts of fiat into virtual assets, or large amounts of one virtual asset type into another, with no logical business explanation.

Anonymity-Related

- Use of services or assets that generate anonymity; virtual assets with a history of mixers or dark web trade.
- Movement from a transparent blockchain to a centralised exchange immediately followed by conversion to an AEC or privacy coin.

- Transfers to or from wallets with patterns associated with mixing, tumbling, or peer-to-peer exchanges.
- Funds with direct or indirect exposure to known suspicious sources: darknet marketplaces, mixing services, gambling sites, ransomware, hacking, or theft.

Customer-Related

- Use of multiple accounts under different names to circumvent trading or withdrawal restrictions.
- Incomplete or insufficient CDD information, or refusal of CDD requests or source-of-funds inquiries.
- Customer's virtual asset address appearing on public forums associated with illegal activity.
- Frequent changes to identification information — email addresses, IP addresses, or financial information — potentially indicating account takeover.
- Source of wealth predominantly derived from virtual asset investments, ICOs, or fraudulent ICOs.
- Forged or edited identification documents submitted during onboarding.

Geographical

- Funds originating from or sent to an exchange not registered in the jurisdiction where the customer or exchange is located.
- Transfers to VASPs operating in jurisdictions with no virtual asset regulation or inadequately implemented AML/CFT controls.

8.2 Actions on Detection

42. Where suspicious activity is detected in relation to an incoming transfer that cannot be stopped due to blockchain processes, VASPs should: restrict the customer's ability to deal with the suspicious funds; freeze assets where technically feasible; and file a report with the FID. VASPs controlling both originating and beneficiary functions must consider information from both sides in determining whether to file. Reports should be filed in the jurisdiction from which the transfer originated or to which it was destined.

9. Virtual Asset Transfers: The Travel Rule

9.1 Originating VASP Obligations

43. Originating VASPs must obtain and hold accurate originator and beneficiary information and transmit it to the beneficiary VASP immediately, simultaneously, or concurrently with the transfer, and in a secure manner that prevents unauthorised disclosure. Required information includes:
    - the originator's name and the beneficiary's name;
    - where an account is used: the account number of the originator and/or beneficiary;
    - the originator's address, IP address, wallet address, government-issued identification document number, customer identification number, or date and place of birth; and
    - where no account is used: the unique transaction reference number permitting traceability.

9.2 Beneficiary VASP Obligations

44. Beneficiary VASPs must obtain and hold required originator and beneficiary information and make it available to appropriate authorities on request. Where required information is missing or incomplete, the beneficiary VASP must either reject the transfer or request the information. Risk-based policies must govern whether to execute, reject, or suspend transfers with incomplete information, and must include internal escalation and external reporting procedures.

45. Where an originating VASP regularly fails to supply required information, the beneficiary VASP must notify it, allow reasonable time for rectification, and document actions taken before restricting or terminating the relationship. Any restriction or termination must be reported to the FID and to the Commission.

9.3 Intermediary VASP Obligations

46. Intermediary VASPs must: maintain documented risk-based policies for handling transfers with missing originator or beneficiary information; ensure all information received accompanies the transfer; and take reasonable measures consistent with straight-through processing to identify deficient transfers.

9.4 Unhosted Wallets

47. Where a VASP receives a transfer from or sends to a non-VASP entity — such as an individual using an unhosted wallet — the VASP must obtain the required originator and beneficiary information from its customer.

9.5 Record Retention

48. All originator and beneficiary information accompanying virtual asset transfers must be retained for a minimum of seven (7) years. Where technical limitations prevent an intermediary VASP from transmitting required information, it must retain all information received for the same period.

9.6 General Compliance

49. VASPs must comply with all relevant requirements in all jurisdictions in which they operate, directly or through agents. Originating VASPs must not execute transfers where required originator and beneficiary information cannot be collected and maintained.