16 VIRTUAL ASSET SERVICE PROVIDERS (VASPS)

16.1 Definition and overview of *VASPs* undertaking *supervised business*

1. Virtual Asset Service Providers (VASPs) are described in Part 4 of Schedule 2 of the Proceeds of Crime (Jersey) Law 1999 defining those services relating to virtual assets that fall under the scope of the *Money Laundering Order*. *Guidelines* provide the interpretation of VASPs and their activities.

2. Due to the fast transfer of value and cross-border transactions, VASPs must mitigate the risks of *money laundering*, *terrorist financing*, *proliferation financing*, and other illicit activities. This section includes specific risks and *money laundering* threats relating to VASPs and other VASP specific guidance.

16.2 VASP specific considerations

Overview

3. VASPs must comply with the same *AML/CTF/CPF* requirements as traditional financial institutions as outlined in Section 1 – 11 of *this Handbook*.

16.2.1 Risk assessment

4. This section is supplemental to, and should be read in conjunction with, Section 3.3.

5. Effective risk assessments and due diligence are essential, particularly when dealing with VASPs exposed to ML/TF/PF risks and foreign VASPs operating in jurisdictions that lack effective *AML/CFT/CPF* frameworks. VASPs should consider avoiding engaging with counterparties that cannot demonstrate effective *AML/CFT/CPF* measures.

6. The use of tools designed to increase anonymity (for example mixers, tumblers, privacy coins and decentralised platforms) increase risk exposure to illicit activities. Additionally, new illicit financing typologies continue to emerge that reduce transparency of transactions that are facilitated by Virtual Assets (VAs) as well as fiat currencies being converted to or from VAs. Therefore, VASPs should take caution to ensure that they investigate suspicious activities and patterns that may indicate emergent risks of ML/TF/PF or other illicit financing risks.

7. VASPs must stay vigilant against being used for layering virtual assets to obscure criminal activities, with risk assessment frameworks being regularly updated to reflect evolving risks.

16.2.1.1 Enhanced due diligence

8. This section is supplemental to, and should be read in conjunction with, Section 7.

9. On a risk basis VASPs are encouraged to collect additional information on high-risk *customer*s and transactions in order to identify, and avoid engaging in, prohibited activities, and to enable follow-up actions. Such additional information may include:

› the purpose of transaction or payment;

› details about the nature, end use or end user of the item;

› proof of funds ownership;

- parties to the transaction and the relationship between parties;
- sources of wealth and/or funds;
- the identity and the beneficial ownership of the counterparty; and
- export control information, such as copies of export-control or other licenses issued by the national export control authorities, and end-user certification.

10. Where a *VASP* is unable to verify the identity of an individual, it should consider not entering into a business relationship or executing a one-off transaction with that individual. If the business relationship already exists, the *VASP* may need to terminate the business relationship. In all circumstances, the *VASP* should consider filing a suspicious activity report in relation to the *customer* or individual.

16.2.2 Travel rule

11. *FATF* has called on jurisdictions to swiftly implement its “Travel Rule.” The Travel Rule requires transfers of virtual assets to be accompanied by accurate originator and beneficiary information. For more information refer to the *Travel Rule Guidance note* on the Jersey Financial Services Commission website.

16.2.3 Blockchain analysis

12. A *supervised person* may implement blockchain analysis to support in meeting their ongoing monitoring commitments as outlined within Section 6 of *this Handbook - Ongoing Monitoring*.

13. Blockchain analysis is a process of investigating, classifying, and monitoring blockchain addresses and transactions to understand the activities of various actors on the blockchain.

14. Blockchain analytics aim to provide transparency into blockchain transactions, including tracking them across different blockchains (i.e., across different crypto assets). They can also support the detection of suspicious activities, understanding transaction patterns, and modelling/visualising data. By analysing and visualising the full chain of transactions, these tools enable investigating entities to trace individual transactions back to identify the original source of funds and assess its legitimacy.

15. As blockchain and associated technologies are considered new and developing, the risks of using such technology to obtain evidence of identity should be considered, noting the particular characteristics of each application. This should be recorded in the BRA.

16. A *supervised person* may wish to implement a suite of monitoring methodologies incorporating new and traditional monitoring measures to ensure they mitigate risks associated with their *customer*s.

16.3 Money laundering typologies

17. Red flag indicators are crucial for detecting and preventing *financial crime* abuse in VASPs. These red flags are non-exhaustive indicative patterns or behaviours that may suggest potential involvement in illicit activities such as *money laundering*, terrorism financing or fraud. By recognising these signs, VASPs may implement effective measures to mitigate risks or cease activity with counterparties.

16.3.1 Red Flag Indicators Related to Transactions

16.3.1.1 Size and frequency of transactions

18. Structuring VA transactions in small amounts or amounts below record-keeping or reporting thresholds, similar to how cash transactions are structured

19. Conducting multiple high-value transactions in quick succession, such as within a 24-hour period, in a staggered and regular pattern, with no further transactions recorded for a long period afterward. This pattern is particularly common in ransomware-related cases or involves newly created or previously inactive accounts.

20. Transferring *VA*s immediately to multiple *VASP*s, especially those registered or operated in jurisdictions unrelated to where the *customer* lives or conducts business, or where *AML/CTF/CPF* regulations are weak or non-existent.

21. Depositing *VA*s at an exchange and then immediately withdrawing them without additional exchange activity, which incurs unnecessary transaction fees. This may also involve converting *VA*s to multiple types of *VA*s, again incurring additional fees without a logical business explanation (e.g., portfolio diversification), or withdrawing *VA*s from a *VASP* immediately to a private wallet. This effectively turns the exchange/*VASP* into a *money laundering mixer*.

22. Accepting funds suspected to be stolen or fraudulent, such as depositing funds from VA addresses identified as holding stolen funds or linked to holders of stolen funds.

16.3.2 Red Flag Indicators Related to Transaction Patterns

16.3.2.1 Transactions concerning new users

23. Making a large initial deposit to establish a new relationship with a *VASP*, where the amount deposited does not align with the *customer*'s profile.

24. Making a large initial deposit to open a new relationship with a *VASP*, funding the entire deposit on the first day, and then either trading/withdrawing the total amount or a significant portion of it on the same day or the next day.

16.3.2.2 Transactions concerning all users

25. Exhibiting abnormal transactional activity, such as high levels and volumes of VAs being cashed out at exchanges without a logistical business explanation.

26. Making frequent transfers to the same VA account within a specific period (e.g. a day, a week, a month) that involves multiple individuals; the same IP address used by one or more individuals; or a large amount of funds.

27. Receiving transactions from numerous unrelated wallets in relatively small amounts, accumulating funds, and then transferring them to another wallet or fully exchanging them for fiat currency. These transactions, conducted by several related accumulating accounts, may initially use VAs instead of fiat currency.

28. Conducting VA-to-fiat currency exchanges at a potential loss, such as when the value of VAs is fluctuating or despite abnormally high commission fees compared to industry standards, especially when there is no logical business explanation for the transactions.

29. Converting a large amount of fiat currency into VAs or converting a large amount of one type of VA into other types of VAs, without any logical business explanation.

16.3.3 Red Flag Indicators Related to Anonymity

30. Customers using multiple types of VAs, especially high anonymity VAs, despite higher transaction fees.

31. Transferring VAs to a centralised exchange and immediately trading them for higher anonymity VAs.

32. Abnormal levels and volumes of VAs cashed out at exchanges from P2P platform-associated wallets without a logical business explanation.

33. VAs transferred to or from wallets with patterns linked to mixing/tumbling services.

34. Transactions using mixing/tumbling services to obscure illicit fund flows.

35. Funds deposited or withdrawn from VA addresses or wallets with links to suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, illegal activities and theft reports.

36. Using decentralised, un-hosted hardware, or paper wallets to transfer VAs across borders.

37. Users registering internet domain names through proxies or using domain name registrars that suppress or redact ownership details.

38. Users accessing VASP platforms using IP addresses associated with darknets or anonymous communication software (such as encrypted emails and VPNs)

39. A large number of seemingly unrelated VA wallets controlled from the same IP or MAC address, potentially using shell wallets registered to different users to conceal their relationship.

40. Using VAs with poorly documented designs or those linked to fraud or fraudulent schemes like Ponzi schemes.

41. Receiving funds from or sending funds to VASPs with weak or non-existent *CDD* processes.

16.3.4 Red Flag Indicators about Senders or Recipients

16.3.4.1 Irregularities observed during account creation

42. Creating multiple accounts under different names to bypass VASP trading or withdrawal limits.

43. Initiating transactions from suspicious or non-trusted IP addresses, including those from sanctioned jurisdictions.

44. Repeatedly attempting to open accounts within the same VASP from the same IP address.

45. Merchants or corporate users registering their internet domains in jurisdictions different from their establishment or in places with a weak domain registration process.

16.3.4.2 Irregularities observed during *CDD* process

46. Providing incomplete or insufficient CDD information or refusing to submit CDD documents or answer questions about source of funds.

47. The sender or recipient lacks knowledge or provide inaccurate information about the transaction, source of funds, or their relationship with the counterparty.

48. Submitting forged documents or altered photographs and identification documents during the onboarding process.

16.3.4.3 Profile of potential money mule or scam victims

49. A sender unfamiliar with VA technology or online custodial wallets.

50. An older *customer*, significantly above the average age of platform users, opens an account and conducts numerous transactions.

51. A financially vulnerable *customer*, often exploited by drug dealers to assist in trafficking activities.

52. A *customer* purchasing large amounts of VAs without substantial wealth or inconsistent with their financial history.

16.3.4.4 Other unusual behaviour

53. A *customer* frequently changes identification details, such as email addresses, IP addresses, or financial information, which may suggest an account takeover.

54. A *customer* attempts to access one or more VASPs from different IP addresses multiple times in a single day.

55. Language in VA message fields indicates transactions supporting illicit activities or the purchase of illegal goods, like drugs or stolen credit card information.

56. A *customer* repeatedly transacts with a specific group of individuals at significant profit or loss.

16.3.5 Red Flag Indicators in the Source of Funds or Wealth

57. Transaction with VA addresses or bank cards linked to fraud, extortion, ransomware, sanctioned addresses, darknet marketplaces, or other illicit website.

58. VA transactions involving online gambling services.

59. Using credit or debit cards linked to a VA wallet to withdraw large amounts of fiat currency or funding VA purchases with cash deposits into credit cards.

60. Deposits into an account or VA address significantly higher than usual with unknown sources, followed by conversion to fiat currency, indicating potential theft.

61. Lack of transparency or insufficient information on the origin and owners of funds, such as those with unavailable investor data, or incoming transactions from online payment systems through credit/pre-paid cards followed by instant withdrawal.

62. Customer funds sourced directly from third-party mixing services or wallet tumblers.

63. A *customer*'s wealth is primarily derived from investments in VAs or ICOs or other VASPs with weak AML/CFT controls.

16.3.6 Red Flag Indicators Related to Geographical Risks

64. Customer's funds are sent to or originate from an exchange not registered in the jurisdiction of either the *customer* or the exchange.

65. Customer uses a VA exchange or foreign-located MVTS in a high-risk jurisdiction or a jurisdiction with inadequate AML/CFT regulations.

66. Customer sends funds to VASPs in jurisdictions without adequate AML/CFT controls or VA regulation.

67. Customer establishes or relocates offices to jurisdictions without adequate AML/CFT controls or VA regulation, or where there is no clear rationale to establish/relocate office in that jurisdiction.

16.4 VASP terminology and glossary

16.4.1 Types of Virtual Assets

Type of Virtual Assets	Description
Utility tokens	VAs that grant digital access to specific digital platforms and to current or planned products or services. Typically, only accepted by the issuer or other users of a particular digital platform.
Payment/exchange tokens	Pseudo-anonymous: used as a means of exchange or potentially as a store of value. Transactions are linked to a specific sender.
	Anonymous (privacy coins): VAs with inbuilt anonymity features. Used as a means of exchange or potentially as a store of value. Transactions are not linked to a specific sender.
	Platform: used to access digital marketplaces and platforms. Also used as a means of exchange and potentially as a store of value.
	Asset-backed tokens (also known as stablecoins): VAs that purport to maintain a stable value by referencing more than one fiat currency, a commodity, or a basket of commodities and fiat currencies.
	Fiat-backed tokens (also known as stablecoins): VAs that purport to maintain a stable value by referencing a single fiat currency.
Closed-loop tokens	VAs used as a means of exchange within a closed system.

16.4.2 Types of Virtual Asset Service Providers

68. The World Bank has defined eight types of virtual asset service providers; however,, two are not defined as VASPs by the FATF. Nevertheless, the entity categories defined in the following table may interact with VAs or VA systems.

Type of Virtual Assets	Description
Wallet providers/custodians	Service providers enabling the storage of public and private keys.
Exchanges	Service providers facilitating virtual asset transfers and exchanges (VA - fiat / fiat - VA / VA - VA).
Payment processors and brokers, including orderbook exchanges	Service providers conducting payment processing/arranging transactions.
OTC desks	Service providers conducting payment processing/arranging transactions.
Asset management providers	Entities offering fund management/fund distribution.
Issuers	Entities issuing and selling VAs to the public.
Investment/trading platforms	Entities enabling investment in or the purchase of VAs via a managed investment scheme or a derivatives issuer providing VA options, or via a private equity vehicle that invests in VAs.

Miners/validators/pool operators*	Entities that validate and confirm transactions on a distributed ledger. Although not usually captured by the VASP definition, if they hold sufficient control/validation power, they could be considered VASPs.
Technology and ancillary service providers*	Entities offering mixing services, blockchain explorers, web administration, mining hosting services, information providers.

*Not covered by FATF recommendations

16.4.3 VASP risk exposure

69. The risks of *money laundering* associated with different types of virtual assets and virtual asset services may be considered as part of *Business Risk Assessment* of a *supervised person*. Example of considerations and higher risk factors is detailed below.

Feature of VA/VASP	Factors which may lead to higher risk of ML abuse
Anonymity	Anonymous Virtual Assets that prevent third parties from linking the VA to an identity.
Accessibility/liquidity	Virtual Assets that are highly liquid and are easily traded/exchanged and provide a more efficient mechanism to exchange or realise value.
Volume of trades	Higher volumes traded lead to higher liquidity levels and a wider range of VAs available to trade.
Amount of deposit/withdrawal	Deposits and withdrawals that involve the movement of larger amounts.
Method of trade	Trading is done via OTC desk (vs. order books). OTC desks may offer higher anonymity and may facilitate one-off transactions that do not require the establishment of a business relationship.
Customers	Private or anonymous individuals/entities rather than, for example, institutional investors and hedge funds.
Exchange used / asset pooling	› Unregulated exchanges used instead of regulated exchanges. › Decentralised exchanges that pool funds (limited traceability) and facilitate peer to peer trading without the governance of an intermediary.
Issuer	Weak controls or lacking AML/CFT processes by issuers allowing easy access to criminals.

70. The above is an example of *money laundering* risks, but VA and VASP services should be assessed by *supervised persons* independently as part of their *Business Risk Assessment*. There is no specific profile in which criminal enterprise abuses Virtual Assets for ML purposes.