Chapter 18
Virtual Assets

Contents of this Chapter

18.1. Introduction

1. The purpose of this Chapter is to provide Virtual Asset Service Providers ("*VASP*s") with guidance on how to meet their obligations within *Schedule 3* and the rules of this *Handbook*, and it contains rules and guidance on the information required to accompany transfers of virtual assets. The guidance in this Chapter is in addition to, and not in place of, the guidance within other chapters of this *Handbook*. *VASP*s fall within the definition of a *specified business* and therefore the *Handbook* is applicable to such firms.

2. The Lending, Credit and Finance (Bailiwick of Guernsey) Law, 2022 was brought into full effect on 1 July 2023 and introduced regulation of *VASP*s to bring *the Bailiwick* in line with international standards, issued by FATF.

3. This Chapter also provides guidance for specified business which are not licensed as *VASP*s but have *business relationships* or *occasional transactions* with a connection to, or involvement with, virtual assets ("*VA*s") – examples where this may arise include where a *customer*'s source of wealth or funds derives from *virtual assets*, or an investment within a structure administered by a *specified business* holds *virtual assets*.

4. *VASP*s are firms which provide or carry out exchange, transfer, safe-keeping, administration, custody, issue, offer, sale, distribution, trading and other activities in connection with *virtual assets* from *the Bailiwick. VASP*s are required to hold a Part III *VASP* licence under the *LCF Law*.

5. The *LCF Law* does not seek to regulate the technology underlying *VA*s or *VASP*s, but rather the natural or *legal person* or *legal arrangement* that may use the technology or software applications to conduct virtual asset services as a business.

18.2. Risk-Based Approach

6. The virtual asset sector is global and the *ML* and *FT* risks facing each business will vary depending on the type of products offered, the *customers* and the delivery channels. The cross-border nature of, potential enhanced-anonymity associated with, and non-face-to-face *business relationships* and transactions facilitated by virtual asset activities (whether licensed or not) could indicate higher risks of *ML* and *FT*, therefore *VASP*s should have appropriate policies, procedures and controls to identify, understand, assess and mitigate these *risks* where applicable.

7. Section 10.2(2) of the Lending, Credit and Finance Rules and Guidance, 2023 prohibits Part III *VASP* licensees from dealing in, trading in, or offering virtual assets or virtual asset services which aim to obscure either the parties to the transaction or the flow of the assets, *VASP*s should therefore consider how they will demonstrate that this is adhered to. For example, *VASP*s should consider whether technological methods have been used to further obfuscate the traceability of *VA* transactions and whether there is technology available to detect such obfuscation.

8. Managing the cybercrime risks and activities to which *VASP*s are susceptible is important and requires the *VASP* to assess and mitigate the cyber risks it faces by establishing appropriate controls to reduce these risks. As *VASP*s are regulated under the Regulatory Laws, they must comply with the Cyber Security Rules and Guidance 2021.

9. Example risk factors specific to virtual assets are included at the end of this Chapter and should be considered by *VASP*s and *specified businesses* involved with virtual asset activities.

18.3 Customer Due Diligence

10. The earlier Chapters in this *Handbook* set forth the required *CDD* measures that *specified businesses* must apply to *business relationships* and *occasional transactions*. These will also apply to *VASP*s. This includes *CDD* measures and where relevant in accordance with Chapter 8 *enhanced measures* and *ECDD*. One notable exception is that, per *Schedule 3* to *the Law,* the designated threshold above which *CDD* must be conducted for an *occasional transaction* in respect of *VASP*s is lower and relates to any transaction or linked transactions involving more than, or to the value of, £1,000.

11. Upon establishing *VASP* operating policies, procedures and controls when accepting *customers* and facilitating transactions, *VASP*s should consider how they will determine if it's a *business relationship* or an *occasional transaction*. It should ensure that an *occasional transaction* is conducted on a one-off or occasional basis, rather than on a more consistent basis. Where a *customer* opens an account with the *VASP*, where an element of duration is likely, it should be considered a *business relationship*.

12. *VASP*s are encouraged to collect additional information to assist them in verifying the *customer*'s identity when establishing a *business relationship* or carrying out an *occasional transaction*; to authenticate the identity of *customers* for account access; to help determine the *customer*'s business and risk profile and conduct ongoing due diligence on the *business relationship*; and mitigate the *ML* and *FT risks* associated with the *customer* and the *customer*'s financial activities. Such additional information could include, for example, an IP address with an associated time stamp, geo-location data, device identifiers, virtual asset wallet addresses and/or transaction hashes. In addition, *VASP*s should also understand whether a *customer*'s virtual wallet address relates to a private wallet, a multi-signature wallet or a custodial wallet.

13. Whilst *VASP*s are required to build a *risk* profile of their *customers*, they should also consider whether a *risk* profile of a cluster of *customers* displaying homogenous characteristics (for example, *customers* conducting similar types of virtual asset transactions or involving the same virtual asset) would be beneficial, for example, to make monitoring via appropriate parameters on monitoring systems easier. Where a cluster of *customers* is identified, the *VASP* should clearly document the criteria and parameters used to allocate *customers* to a cluster.

14. As part of a *VASP*'s ongoing monitoring, it should screen its *customers*' and counterparties' wallet addresses against available blacklisted wallet addresses, adverse media and sanctions and determine whether mitigation or preventive actions are warranted in the event of a positive hit. Where available, *VASP*s should use analytical tools available to them to detect potentially fraudulent transactions and other suspicious activity, for example, that the *VA*s were used on the dark web or in connection with a ransomware attack. Where this is not possible this should increase the *risk* profile of the *customer*.

15. Where a *VASP* is undertaking source of wealth verification and where the source of wealth disclosed is from mining or staking virtual assets, documentation on the mining operation could be through the collection of electricity bills and hardware receipts etc. and an assessment should be made as to whether the *customer* can afford to run the mining operation given their declared source of wealth. Documentation on the staking could be via the smart contract entered into for the staking, or through analysis of the *customer'*s blockchain address. Where money has been paid out from a mining or staking pool, the *VASP* should obtain evidence that the address from which the *VA*s were transferred is controlled by a mining or staking pool and that the *customer* had a connection with the mining or staking pool.

16. Where funds are being returned due to insufficient *CDD*, they must be returned to the same account they were paid from and should be accompanied with script stating they are being refunded due to

the inability to complete *CDD*. Where this is the case, consideration should be given to making a disclosure to the *FIU* in accordance with Chapter 13 on reporting suspicion.

17. When transaction information is easily available on a public ledger or via other open sources, *VASP*s must still record and retain that information in accordance with Chapter 11 on monitoring transactions and activity.

18.4. Enhanced Customer Due Diligence

18. There are *ECDD* measures which can be undertaken in relation to *VA*s in addition to those already included within Chapter 8 on *enhanced customer due diligence*. Examples of additional steps the firm could take when meeting the requirements of Paragraphs5(3)(v)(A)-(D) of *Schedule 3* while undertaking *ECDD* in relation to *VA*s could include, but is not limited to, applying one or more of the following measures most relevant towards mitigating the *ML* risks:

(a) corroborating the identity information received from the *customer*, such as a national identity number, with information in third-party databases or other reliable sources;
(b) tracing the *customer*'s IP address;
(c) using analysis products;
(d) using open source to corroborate activity information consistent with the *customer*'s transaction profile; and/or
(e) collecting additional information on:
   i. the purpose of the transaction or payment;
   ii. details about the nature, end use or end user of the item;
   iii. proof of funds ownership;
   iv. parties to the transaction and the relationship between the parties;
   v. the identity and beneficial ownership of the counterparty; and
   vi. export control information, such as copies of export control or other licenses issued by a national export control authority, and end user certification.

18.5. Correspondent Banking and Other Similar Relationships

19. Correspondent banking (the provision of banking services by one *bank* to another *bank*) and other similar relationships do not include one-off transactions, but instead are characterised by their ongoing, repetitive nature. *VASP*s should define and assess the characteristics of their counterparty *VASP* relationships and ascertain whether they are undertaking activities similar to correspondent banking. Where it is established that a *VASP* is entering into a relationship that is similar to correspondent banking, it should adhere to the rules and guidance included within Section 8.6 of this *Handbook* on correspondent banking.

18.6. Transfers

20. *VASP*s are required to obtain, hold and submit required originator and beneficiary information associated with the transfers of virtual assets in order to identify and report suspicious transactions, take freezing actions and prohibit transactions with designated persons and entities. This is similar to the *wire transfer* requirements included within Chapter 14.

21. *The Commission* does not require a particular technology or software to be used to comply with the transfer rules. Any technology or software used must enable the originator and beneficiary *VASP*s to comply with their AML/CFT obligations.

22. The technology or software used should enable *VASP*s to comply with the transfer rules in an effective and efficient manner and enable *VASP*s to undertake the following actions:

a) Enable a *VASP* to locate counterparty *VASP*s for transfers of virtual assets;
b) Enable the submission of required and accurate originator and required beneficiary information immediately when a virtual asset transfer is conducted on a distributed ledger technology platform;
c) Enable *VASP*s to submit reasonably large volume of transactions to multiple destinations in an effectively stable manner;
d) Enable a *VASP* to securely transmit data, i.e., protect the integrity and availability of the required information to facilitate record-keeping;
e) Protect the use of such information by receiving *VASP*s or other entities involved with virtual assets as well as to protect it from unauthorised disclosure in line with Guernsey data protection legislation;
f) Provide a *VASP* with a communication channel to support further follow-up with a counterparty *VASP* for the purpose of:

(i) Due diligence on the counterparty *VASP*; and
(ii) Requesting information on a certain transaction to determine if the transaction involved high risk or prohibited activities.

18.6.1 Transfers of virtual assets to a beneficiary – Originating *VASP* obligations

23. In accordance with Paragraph 15C(1) of *Schedule 3*, in respect of any virtual asset transfer, an originating *VASP* shall –

(a) obtain and hold required and accurate originator information and required beneficiary information,
(b) ensure that the information specified in (a) accompanies the transfer of the virtual asset to the beneficiary *VASP* immediately and securely,
(c) make the information specified in (a) available on request to *the Commission* and other appropriate authorities as soon as is reasonably practicable,
(d) not execute any virtual asset transfer in respect of which (b) is not complied with, and
(e) in the case of a transaction which would be an *occasional transaction* but for the sum involved being £1,000 or less, obtain and hold such information, or information of such class or description, as may be specified for the purposes of this Part of this Schedule in requirements set out in *the Handbook*.

24. When conducting a *VA* transfer, the originating *VASP* must ensure that *VA* transfers are accompanied by the following originator information:

(a) the name of the originator;
(b) where a transfer of *VA*s is registered on a network using distributed ledger technology or similar technology, the originator's distributed ledger address and the originator's *VA* account number, where such an account exists and is used to process the transaction;
(c) where a transfer of *VA*s is not registered on a network using distributed ledger technology or similar technology, the originator's account numbers;
(d) where a transfer of *VA*s is neither registered on a network using distributed ledger technology or similar technology nor is made from or to a *VA* account, the originator *VASP* shall ensure that the transfer of *VA*s is accompanied by a unique transaction identifier which permits traceability of the transaction;
(e) one of either:
(i) the originator's address, including the name of the country,
(ii) national identity number,
(iii) *customer* identification number or
(iv) date and place of birth; and

(f) subject to the existence of the necessary field in the relevant message format, and where provided by the originator to the originator's *VASP*, the current Legal Entity Identifier ("LEI") of the originator or any other available equivalent official identifier.

25. Where the *originator* is an existing *customer* of the *VASP* to whom it should have applied due diligence measures consistent with this *Handbook*, the *VASP* may deem verification to have taken place if it is appropriate to do so taking into account the risk of *ML* and *FT*.

26. A national identity number should be any government issued personal identification number or other government issued *unique identifier*. Examples of such would include a passport number, national identity card number or social security number.

27. A *customer* identification number may be an internal reference number that is created by a *VASP* which uniquely identifies a *customer* (rather than an *account* that is operated for an *originator* or a transaction) and which will continue throughout a *business relationship*, or it may be a number that is contained within an official document.

28. Prior to conducting the *VA* transfer, the originating *VASP* must verify the accuracy of the information obtained in Commission Rule 18.24(a), (e) and (f) using documents, data or information obtained from a reliable and independent source.

29. When conducting a *VA* transfer, the originating *VASP* must ensure that *VA* transfers are accompanied by the following beneficiary information:

(a) the name of the beneficiary;
(b) where a transfer of *VA*s is registered on a network using distributed ledger technology or similar technology, the beneficiary's distributed ledger address and the beneficiary's *VA* account number, where such an account exists and is used to process the transaction;
(c) where a transfer of *VA*s is not registered on a network using distributed ledger technology or similar technology, the beneficiary's account numbers;
(d) where an account is not used to process the transfer, the unique transaction identifier which permits the traceability of the transaction; and
(e) subject to the existence of the necessary field in the relevant message format, and where provided by the originator to the originator's *VASP*, the current LEI of the originator or any other available equivalent official identifier.

30. The information referred to in Commission Rules 18.24 and 18.29 should be submitted in advance of, or simultaneously or concurrently with, the transfer of *VA*s and in a secure manner that complies with *the Data Protection Law*. It does not have to be attached directly to, or be included in, the transfer of *VA*s.

31. Where a *VA* transfer is made to a self-hosted address, the originating *VASP* must obtain and hold information referred to in Commission Rules 18.24 and 18.29 and ensure that the *VA* transfer can be individually identified.

32. Where a *VA* transfer in excess of £1,000 is made to a self-hosted address, the originating *VASP* must take adequate measures to assess if such address is owned or controlled by the originator.

33. An originating *VASP* must not execute a transfer where it is unable to collect and maintain the required information referred to in Commission Rules 18.24 and 18.29.

34. Where a transfer is carried out which is at, or below, the £1,000 threshold, the originating *VASP* must obtain and hold:

a) the name of the originator and the beneficiary; and
b) the *VA* wallet address for each or a unique transaction reference number,

but it is not necessary to verify the *customer* information on the originator unless the virtual assets to be transferred have been received anonymously, or the *VASP* has reasonable grounds for suspecting *ML* and/or *FT*.

18.6.2 Batch Transfers

35. In accordance with Paragraph 15E of *Schedule 3*, in the case of a batch transfer, an originating *VASP* shall –

(a) ensure that the batch file contains required and accurate originator information and required beneficiary information,
(b) ensure that the information specified in (a) is such as to permit the traceability within the beneficiary jurisdiction of each transaction comprised in the batch from the originator to the beneficiary (and "beneficiary jurisdiction" means the jurisdiction in which the beneficiary *VASP* received the transfer of the virtual assets), and,
(c) include the originator's account number or unique transaction identifier and/or such other information, or information of such a class or description, as may be specified in *the Handbook*.

36. The batch file information requirements which apply where several individual *VA* transfers with a single originator are bundled together for transmission in a batch transfer include:

(a) the name of the originator;
(b) where an account is used to process the transfer of *VA*s by the originator, the account number of the originator;
(c) one of either
(i) the originator's address, including the name of the country,
(ii) national identity number,
(iii) *customer* identification number or
(iv) date and place of birth;
(d) the individual transfers of *VA*s carry the account number of the originator or a unique identifier; and
(e) the name, account number or unique identifier of the beneficiary that is traceable in the beneficiary country.

37. Where a batch transfer is carried out which is at, or below, the £1,000 threshold, the originating *VASP* must obtain and hold:

a) the name of the originator and the beneficiary; and
b) the *VA* wallet address for each or a unique transaction reference number,

but it is not necessary to verify the *customer* information on the originator unless the virtual assets to be transferred have been received anonymously, or the *VASP* has reasonable grounds for suspecting *ML* and/or *FT*.

18.6.3 Transfers of virtual assets to a beneficiary – Beneficiary *VASP* obligations

38. In accordance with Paragraph 15C(2) of *Schedule 3*, in respect of any virtual asset transfer, a beneficiary *VASP* shall –

    (a) obtain and hold required and accurate beneficiary information and required originator information,
    (b) make the information specified in (a) available on request to *the Commission* and other appropriate authorities as soon as is reasonably practicable,
    (c) in the case of a transaction which would be an occasional transaction but for the sum involved being £1,000 or less, obtain and hold such information, or information of such class or description, as may be specified for the purposes of this Part of this Schedule in requirements set out in *the Handbook*.

39. On receipt of a *VA* transfer, the beneficiary *VASP* must ensure that *VA* transfers are accompanied by the following originator and beneficiary information:

    (a) the name of the originator and the beneficiary;
    (b) the account numbers of the originator and the beneficiary, where an account is used to process the *VA* transfer;
    (c) the address of the beneficiary, the number of a government-issued document evidencing the beneficiary's identity, *customer* identification number or date and place of birth; and
    (d) where an account is not used to process the transfer, the unique transaction identifier which permits the traceability of the transaction.

40. Further rules and guidance relating to transfers with missing or incomplete information is included within Section 18.6.4.

41. Prior to making the *VA*s available to the beneficiary, the beneficiary *VASP* must verify the accuracy of the above information regarding the beneficiary of the transfer, using data or documentation.

42. Where a *VA* transfer is made to a self-hosted address, the beneficiary *VASP* must obtain and hold information referred to in Commission Rule 18.39 and ensure that the *VA* transfer can be individually identified.

43. Where a *VA* transfer in excess of £1,000 is made to a self-hosted address, the beneficiary *VASP* must take adequate measures to assess if such address is owned or controlled by the beneficiary.

44. Where a transfer is carried out which is at, or below, the £1,000 threshold, the beneficiary *VASP* must obtain:

    a) the name of the originator and the beneficiary; and
    b) the *VA* wallet address for each or a unique transaction reference number,

    but it is not necessary to verify the *customer* information on the originator unless the virtual assets to be transferred have been received anonymously, or the *VASP* has reasonable grounds for suspecting *ML* and/or *FT*.

18.6.4 Transfers of *VA*s with missing or incomplete information on the originator or the beneficiary

45. In accordance with Paragraph 15D of *Schedule 3*, a beneficiary *VASP* shall –

    (a) before making a virtual asset available to a beneficiary –

(i) monitor the completeness of the originator information, and
(ii) take remedial action where the information specified in (i) is incomplete,

(b) have risk-based policies for –

(i) determining when to reject, suspend or otherwise refuse to execute virtual asset transfers because of information deficiencies, and
(ii) the taking of appropriate follow-up action, and

(c) report to *the Commission* repeated failures by an originating *VASP*, beneficiary *VASP* or intermediary *VASP* to comply with the requirements of *Schedule 3* as to the obtaining, holding, verification, retention, provision and use of information in respect of virtual asset transfers.

46. The beneficiary *VASP* must have effective procedures and/or systems in place to detect whether the required information is obtained on a *VA* transfer and to detect missing information on both the originator and the beneficiary.

47. The beneficiary *VASP*'s policies, procedures and controls should:

(a) take into account the *ML* and *FT risks* to which it is exposed;
(b) set out which transfers will be monitored in real time and which can be monitored ex-post and why; and
(c) set out what *employees* should do where the information is missing or incomplete.

48. The level of monitoring should be appropriate to the *risk* of the *VASP* being used in connection with *ML* or *FT,* with high *risk* transfers monitored in real time.

49. Where the beneficiary *VASP* becomes aware that the information is missing or incomplete, the beneficiary *VASP* must, prior to making the *VA*s available to the beneficiary:

(a) ask for and obtain the required information on the originator and the beneficiary;
(b) reject the transfer prior to the *VA*s being received; or
(c) return the transferred *VA*s to the originator's *VA* account if already received.

50. Where a *VASP* repeatedly fails to provide the required information on the originator or the beneficiary, the beneficiary *VASP* must:

(a) take steps to obtain the required information, including, but not limited to,
(i) the issuing of a warning and setting of deadlines;
(ii) reject any future transfers from, or to, a *VASP* that fails to provide the required information, and/or
(iii) restrict or terminate its business relationship with a *VASP* that fails to provide the required information; and
(b) notify *the Commission* of that failure and which of the above steps it has taken.

18.6.5 Intermediary *VASP*s

51. In accordance with Paragraph 15C(3) of *Schedule 3*, in respect of any virtual asset transfer, an intermediary *VASP* shall –

(a) take reasonable measures which are consistent with straight-through processing to identify transfers received by it that are not accompanied by the originator and beneficiary information specified in 15C(1)(a),

(b) report to *the Commission* repeated failures by an originating *VASP*, beneficiary *VASP* or intermediary *VASP* to comply with the requirements of *Schedule 3* as to the obtaining, holding, verification, retention, provision and use of information in respect of virtual asset transfers,

(c) ensure that any beneficiary information and originator information accompanying the transfer is retained with it,

(d) subject to (e), ensure the information specified in (c) accompanies the onward transfer that the intermediary *VASP* will be making,

(e) where technical limitations prevent the information specified in (c) from accompanying an onward transfer, keep a comprehensive record of all information received from the originating *VASP* or another intermediary *VASP* for a period of not less than five years starting from the date of receipt of the virtual asset by the intermediary *VASP*, and

(f) have risk-based policies for:

(i) determining when to reject, suspend or otherwise refuse to execute virtual assets transfers because of information deficiencies, and
(ii) the taking of appropriate follow-up action.

52. In respect of any virtual asset transfer, an intermediary *VASP* must:

(a) implement effective procedures including, where appropriate, monitoring after or during transfers, to detect whether the information on the originator or the beneficiary is submitted previously, simultaneously or concurrently with the *VA* transfer or batch file transfer, including where the transfer is made from or to a self-hosted address; and

(b) take reasonable measures to identify transfers which lack required originator or beneficiary information.

53. Where the intermediary *VASP* becomes aware that the information is missing or incomplete, the *VASP* must, prior to making the *VA* transfer:

(a) reject the transfer and return the transferred *VA*s where in the intermediary *VASP*'s possession; or

(b) ask for and obtain the required information on the originator and the beneficiary.

54. Where a *VASP* repeatedly fails to provide the required information on the originator or the beneficiary, the intermediary *VASP* must:

(a) take steps to obtain the required information, including, but not limited to,
(i) the issuing of a warning and setting of deadlines;
(ii) reject any future transfers from, or to, a *VASP* that fails to provide the required information, and/or
(iii) restrict or terminate its business relationship with a *VASP* that fails to provide the required information; and

(b) notify *the Commission* of that failure and which of the above steps it has taken.

18.6.6 Record retention

55. Both the originating *VASP* and the beneficiary *VASP* must keep records of the complete originator and beneficiary information for each *VA* transfer for at least five years.

56. In addition, where technical limitations prevent an intermediary *VASP* from sending the required originator or beneficiary information with a *VA* transfer, the intermediary *VASP* must keep records of all information received for at least 5 years.

18.7. Reporting

57. Irrespective of the capacity within which the *VASP* is acting, i.e. originator *VASP*, beneficiary *VASP* or intermediary *VASP*, there are three distinct reporting requirements which are that:

    (a) missing or incomplete information on a transfer which may give rise to a suspicion of *ML* or *FT* where that suspicion should be reported to the *FIU*;
    (b) breaches by a *VASP* of the requirements of paragraphs 15C, 15D or 15E of Schedule 3 and rules in the *Handbook* should be reported to *the Commission*; and
    (c) repeated failure by a *VASP* to provide the required originator or beneficiary information should be reported to *the Commission*.

18.7.1. Reporting Suspicions and Sanction screening

58. Beneficiary and intermediary *VASP*s should take into account missing or incomplete information on the originator or the beneficiary as a factor when assessing whether a *VA* transfer, or any related transaction, is suspicious and whether it is to be reported to the *FIU*. For further information on reporting suspicion, reference should be made to Chapter 13 of this *Handbook* on reporting suspicion.

59. *VASP*s should implement mechanisms to ensure that transactions are scrutinised effectively to identify any suspicious transactions to report to the FIU and screening transactions to meet sanctions obligations to report to the Policy and Resources Committee, as required (see chapter 12 on sanctions). *VASP*s should consider reviewing a combination of the other *customer* information, transaction history and additional transaction data obtained either from the *customer* directly, or from the counterparty *VASP* within the implemented mechanisms.

60. *The Commission* would expect the *VASP*'s internal reporting procedures to apply where an *employee* of a *VASP* forms a suspicion that a transfer may be connected to *ML* and/or *FT*, or that funds are derived from the *proceeds* of crime or are terrorist property.

61. *Employees* who are involved in the handling or processing of transfers would be considered *relevant employees* for AML/CFT training purposes and a *VASP* should ensure that its training programme includes training to meet the requirements of Chapter 15 on employee screening and training in this *Handbook*, as well as the *VASP*'s policies, procedures and controls on handling transfers of funds and reporting suspicion.

18.7.2. Reporting Breaches

62. A *VASP* must establish policies and procedures for the internal reporting by *employees* of breaches of this *Handbook*, and maintain a record of those breaches and action taken. Such policies and procedures must ensure sufficient confidentiality and protection for *employees* who report breaches committed within the *VASP*.

63. The *board* of a *VASP* should consider notifying *the Commission* in accordance with the requirements of *Commission Rule* 2.49 of any failure by it (the *VASP*) to comply with this *Handbook*.

64. Notifications to *the Commission* should be made promptly and contain the following information:

    (a) the specific provision in this *Handbook* and all of the *VASP*'s policies, procedures and controls which have been breached;
    (b) the nature of the breach, including its cause;
    (c) the date the breach was identified by the *VASP*; and

(d) where possible a summary of the measures taken by the *VASP* in relation to the breach and any subsequent changes to its policies, procedures and controls to mitigate against a recurrence.

65. In order to ensure that the breach is reported promptly, a *VASP* should consider filing an initial report covering items (a) to (c) in Paragraph 18.64 above, together with the steps it is considering taking under (d).

18.8. Risks Associated with the Virtual Assets Sector

66. Due to certain characteristics, such as anonymity, immediacy with which a *virtual asset* can be transferred, ease, irrevocability and decentralisation, *VA*s are often associated with illicit activities and *ML* as well as providing an additional means for *FT* and *PF*. Furthermore, the nature of this payment service means that as well as establishing *business relationships* with their *customers*, *VASP*s also carry out *occasional transactions*, where their understanding of the *ML* and *FT risk* associated with the *customer* may be limited because there is no ongoing relationship.

67. Decentralised *VASP*s have no central oversight body. AML compliance software is being developed to monitor and identify suspicious transaction patterns, but is not yet commercially tested and available. Conversely, software products have been developed to enhance decentralised *VASP*s' anonymity features, including coin mixers and IP address anonymisers and the use of these tools may make application of *CDD* measures nearly impossible.

68. *VASP*s should be aware of the following *risk* factors alongside those set out in Paragraph 3 of *Schedule 3* and Chapter 3 of this *Handbook*.

18.8.1 Product, Service and Transaction Risk Factors

69. The following factors may contribute to increasing *risk*:

(a) transactions are often fast, simple and irreversible;
(b) the product or service has a global reach, including to high risk jurisdictions or potentially to breach sanctions;
(c) the transaction is cash-based, involves *VA*s or is funded with anonymous electronic money and does not necessarily rely upon other regulated entities;
(d) products are largely unregulated in many jurisdictions;
(e) where *occasional transactions* are undertaken, they take place outside of an established *business relationship* that could otherwise be more readily monitored for uncharacteristic behaviour;
(f) products and techniques that can be used to facilitate anonymity (AECs, mixing and tumbling services, clustering of wallet addresses and privacy wallets), or to exploit a false identity;
(g) transactions that appear to have no obvious economic or financial basis;
(h) unusual, complex or uncharacteristically large transactions;
(i) transactions that route through third countries or third parties, including mixers;
(j) transactions that can be traced to or from the dark web or mixing/tumbler services;
(k) transactions accompanied by information that appears false or contradictory;
(l) transfers to the same person from different individuals or to different persons from the same individual with no reasonable explanation;
(m) decentralised *VASP*s are particularly vulnerable to anonymity risks, e.g. by design, certain *VA* wallet addresses that function as accounts, may have no names or *customer* identification attached and the system may have no central server or service provider;
(n) historical transaction chains generated on blockchain are not necessarily associated with the identified *customer*;
(o) transactions can present challenges in tracing the flow of *VA*s and freezing or seizing illicit proceeds held as *VA*s due to data encryption;

(p) *VA*s are deposited soon after registration and withdrawn again shortly after without making use of the services/products of the *VASP*, or are deposited and left dormant;

(q) transactions are conducted that are inconsistent with reasonable trading patterns/strategies, or at specific times and amounts that are not in line with normal industry practices; and/or

(r) the holder of a private key in relation to *VA*s is able to control and transfer the *VA*s at any given point in time, the holder of the private key can change and therefore makes the private key similar to a bearer instrument. As such, risks relating to bearer instruments are applicable to *VA*s.

18.8.2 Customer Risk Factors

70. The following factors may contribute to increasing *risk*:

(a) the *customer's* business activity:

(i) the *customer* owns or operates a business that handles large amounts of cash or *VA*s; and/or

(ii) the *customer's* business has a complicated ownership structure.

(b) the *customer's* behaviour:

(i) the *customer's* needs may be better serviced elsewhere, for example, because the *VASP* is not local to the *customer* or the *customer's* business;

(ii) the *customer* offers false, fraudulent or fictitious identification information or documents;

(iii) the *customer* delays producing identification documents or other requested information without suitable justification, or cancels a transaction after learning of a *CDD* requirement;

(iv) the *customer's* behaviour makes no apparent economic sense, for example, the *customer* accepts a poor exchange rate or high charges unquestioningly, requests a transaction in a currency that is not official tender or commonly used in the jurisdiction where the *customer* and/or recipient is located or requests or provides large amounts of currency in either low or high denominations;

(v) the *customer's* transactions are always just below applicable thresholds, including the £1,000 threshold for *occasional transactions* set out in *the Law*;

(vi) the *customer's* use of the service is unusual, for example, they send or receive *VA*s to or from themselves or send *VA*s on immediately after receiving them;

(vii) the *customer* appears to know little or is reluctant to provide information about the beneficiary;

(viii) several of the firm's *customers* transfer *funds* to the same beneficiary or appear to have the same identification information, for example, address or telephone number;

(ix) an incoming transaction is not accompanied by the required information on the originator or beneficiary;

(x) the amount sent or received is at odds with the *customer's* income (if known);

(xi) the *customer* makes use of mixing/tumbler services or similar, or engages in transactions that can be traced to the dark web;

(xii) the *customer* is a legal person which cannot be found on the internet and/or uses an email address with an unusual domain part such as Hotmail, Gmail, Yahoo etc. especially if the *customer* is otherwise secretive or avoids direct contact;

(xiii) the *customer* uses proxies or unverifiable IP addresses or uses disposable email addresses or mobile numbers;

(xiv) the *customer* uses different devices to conduct transactions to obscure their actual location or circumvent restrictions;

(xv) the *customer* uses multiple wallets for the same virtual assets or changes wallets for the same virtual asset;

(xvi) the *customer* is a business or NPO which transacts with the *VASP* in a manner expected of individuals, which could indicate a front or shell company or be indicative of misappropriation of funds;

(xvii) the *customer*'s IP address either appears to be connected to a VPN or other similar IP anonymisers, changes repeatedly, or does not agree to other information held by the firm on the c*ustomer*'s location;

(xviii)the *customer* is part of a complex structure that makes the determination of the beneficial owner more difficult; and/or

(xix) the bank account or payment card linked to the *customer*'s account is changed often.

18.8.3 Country or Geographical Risk Factors

71. The following factors may contribute to increasing *risk*:

(a) The originator or the beneficiary is located in a jurisdiction associated with higher *ML* and/or *FT risk*;

(b) The beneficiary is resident in a jurisdiction that has no, or a less developed, formal banking sector, which means that informal money remittance services, such as hawala, may be used at point of payment;

(c) *VASP*s based in other jurisdictions may not require a user to be identified and their identity verified; and/or

(d) *VASP*s based in other jurisdictions may not be regulated, or may have regulatory requirements that do not meet, or insufficiently meet, FATF Standards.

18.8.4 Distribution Channel Risk Factors

72. The following factors may contribute to increasing *risk*:

(a) there are no restrictions on the funding instrument, for example, cash, unrestricted E-money products, *wire transfers*, cheques or *VA*s;

(b) there is a lack of face-to-face contact with the *customer* and any persons associated with them;

(c) the distribution channel used provides a degree of anonymity;

(d) the service is provided entirely online without adequate safeguards;

(e) the *VA* service is provided through agents that:

(i) represent more than one principal;

(ii) have unusual turnover patterns compared with other agents in similar locations, for example, unusually high or low transaction sizes, unusually large cash transactions or a high number of transactions that fall just under the *CDD* threshold, or undertake business outside normal business hours;

(iii) undertake a large proportion of business with originators or beneficiaries from jurisdictions associated with higher *ML* and/or *FT risk*;

(iv) appear to be unsure about, or inconsistent in, the application of group-wide AML and CFT policies; or

(v) are not from the financial sector and conduct another business as their main business;

(f) the *VA* service is provided through a large network of agents in different jurisdictions; and/or

(g) the *VA* service is provided through an overly complex payment chain, for example, with a large number of intermediaries operating in different jurisdictions or allowing for untraceable (formal and informal) settlement systems;