14 *WIRE TRANSFERS AND PREPAID CARDS*

14.1 Wire transfers

14.1.1 Overview of section

1. The *Wire Transfers Regulations* were brought into force on 13 June 2017, following the EU's enactment of the *EU Regulation* on 20 May 2015. It implements *FATF Recommendation* 16 and promotes an enhanced framework around the traceability of transfers of funds for the purpose of preventing, detecting and investigating *money laundering,* the *financing of terrorism,* or the *financing of proliferation* and other *financial crime*s.

2. The *EU Regulation* expanded the regulatory requirements with the following objectives:

- to prevent the abuse of fund transfers for *money laundering*, *terrorist financing* and other *financial crime* purposes;
- to detect such abuse should it occur;
- to support the implementation of restrictive measures; and
- to allow *supervised* authorities to access the information promptly.

3. In this section, any reference to a numbered Article, without further detail, is a reference to the Article so numbered inf the EU Regulation.

Statutory Requirements (paraphrased wording)

4. ***Regulation 2 of the Wire Transfers Regulations gives the EU Regulation full force and effect, subject to certain adaptations, exceptions and modifications as set out in its Schedule 1.***

5. *Under the Wire Transfer Regulations, the following definitions apply:*

6. *"money or value transfer service provider" **(MVTS)** means a person who provides a money or value transfer service within the meaning given in paragraph 5 in Part 2 of* Schedule 2 *of the Proceeds of Crime (Jersey) Law 1999.*

7. *"payment service provider" (**PSP**) means a person, being a person registered under the BB(J) Law, or who is a VASP or a MVTS, when:*

- *the person is carrying out payment services in or from within Jersey; or*
- *being a legal person established under Jersey law, the person is carrying out payment services in any part of the world other than in or from within Jersey.*

8. *"intermediary payment service provider" (**IPSP**) means a PSP that is neither that of the payer nor that of the payee and that participates in the execution of transfers of funds;*

9. *"payer" means a person that is the holder of an account held with a PSP that allows a transfer of funds or value from the account or, where there is no account, a person that places an order for a transfer of funds;*

10. *"payee" means a person that is the intended final recipient of transferred.*

11. *"virtual asset" has the meaning given in Part 1 of* Schedule 2 *to the law.*

12. *"virtual asset service provider" **(VASP**) has the meaning given in Part 4 of* Schedule 2 *to the law.*

13. Article 2*A(1)* of the Wire *Transfer* Regulations, *states that* Article 2 of the Wire Regulations shall not apply *(and hence the EU Regulations do not apply)* to transfers of virtual assets equivalent to less than EUR 1,000.00 if the payer and payee are both *VASPs*.

14. *D*espite any other stipulation under the EU Regulations*, Article 2A(2) of the* Wire Transfer *R*egulations *requires that if* a payment service provider considers that there is a higher risk of *money laundering* in respect of virtual assets *then it* must comply with Article 2 of the Wire Transfer Regulations *(and hence the EU Regulations)* irrespective of the amount transferred if:

- *the payer is a VASP and the payee is not a VASP; or*
- *the payer is not a VASP and the payee is a VASP.*

Guidance notes

15. The core requirement is that every wire transfer must be accompanied by specific information (**complete information**) about the payer and the payee, which should be collected and retained by payment service provider or intermediary payment institutions, unless special exemptions and derogations apply, including funds transfers between the British Islands (referred in this section as being the *UK*, Jersey, Guernsey, and the Isle of Man).

16. A PSP should establish for each transfer of funds whether it acts as the PSP of the payer, the payee or as an IPSP. This will determine what information must accompany a transfer of funds and the steps required to comply with the *Wire Transfer Regulations*.

17. The *Wire Transfer Regulations* also require PSPs to put in place effective procedures to detect transfers of funds that lack the required information about the payer and the payee, and to determine whether to execute, reject or suspend such transfers of funds.

18. In line with the Data Protection (Jersey) Law 2018, personal data obtained by PSPs should be used only for the purpose of preventing *money laundering*, *terrorist financing,* or *proliferation financing*. PSPs should ensure the confidentiality of such data.

19. Any record of information on the payer/payee should not be kept longer than is necessary for the purposes of preventing, detecting, and investigating *money laundering,* the *financing of terrorism,* or the *financing of proliferation*.

20. Outside the normal data collection PSPs are expected to record information on the payer or payee. However, *Article 2A* of the *Wire Transfer Regulations* gives *PSPs* an exemption for transfers worth less than a €1000.00 between VASPs.

21. This exemption falls away if either the payer or payee is not a VASP, and the payment is high risk for *money laundering*. As such, *PSPs* must apply the *EU Regulations* as adopted into law, as per Article 2 of the *Wire Transfer Regulations.*

22. The risk factors to be considered are as stated under section 3.3.4.1 of *this Handbook*, in the cases highlighted at sections 4.3 and 4.5 of *this Handbook*.

23. The JFSC will be issuing a Guidance Note detailing the requirements for proprietary, inter-entity, Jersey-to-Jersey and inter-group transfers. The Guidance Note will also provide a steer on the suggested approach to the transfer of funds to unregulated VASPs in foreign jurisdictions.

24. The JFSC acknowledges that the process of integrating these requirements into a business' practice may take time. Supervision teams would expect that VASPs take reasonable steps towards the implementation of a solution and subsequent compliance with these requirements.

14.1.2 Scope of the Wire Transfer Regulations

Overview

Statutory requirements (paraphrased wording)

25. *Under Article 1 the EU Regulation, the Wire Transfers Regulations shall apply to transfers of funds, in any currency, which are sent or received by PSP or IPSP established in Jersey. These apply to credit transfers, direct debits, money remittances and transfers carried out using a payment card, an electronic money instrument, or a mobile phone, or any other digital or IT prepaid or post-paid device with similar characteristics, irrespective of whether the payer and the payee are the same person and irrespective of whether the PSP of the payer and that of the payee are one and the same. For British Islands-based PSPs, it includes, but is not necessarily limited to, international payment transfers made via SWIFT, including various Euro payment systems, and domestic transfers via CHAPS and BACS.*

26. *Article 2(2) provides the reference to exclusions from the scope of the Wire Transfer Regulations.*

27. *The Wire Transfer Regulations shall not apply to transfers of funds that represent a low risk of money laundering or the financing of terrorism under Article2(4), such as:*

- *transfers of funds, that involve the payer withdrawing cash from the payer's own payment account;*
- *transfers of funds to a public authority as payment for taxes, fines or other levies within the British Islands;*
- *transfers of funds where both the payer and the payee are PSPs acting on their own behalf;*
- *transfers of funds carried out through cheque images exchanges, including truncated cheques.*

28. *By way of exception, under Article 2(3), the EU Regulation shall not apply to transfers of funds carried out using payment cards, electronic money instruments, mobile phones or other digital or information technology (IT) prepaid or post-paid devices with similar characteristics, where the following conditions are met:*

a) that card, instrument or device is used exclusively to pay for goods or services; and

b) the number of the card, instrument or device accompanies all transfers flowing from the transaction.

29. *By way of derogation, under Article 2(5) the EU Regulation, the Wire Transfer Regulations shall not apply to transfers of funds within the British Islands to a payee's payment account permitting payment exclusively for the provision of goods and services where all the following conditions are met:*

a) the PSP of the payee is subject to the requirements of the Money Laundering Order or the Terrorism Law or is subject to equivalent requirements under enactments of the UK, Guernsey or the Isle of Man;

b) the PSP of the payee is able to trace back, through the payee, by means of a unique transaction identifier, the transfer of funds from the person who has an agreement with the payee for the provision of goods or services;

c) the amount of the transfer of funds does not exceed €1,000.

Guidance notes

30. A *supervised person* should have in place *systems and controls* (including *policies and procedures*) to ensure the conditions for the exemptions and derogations are met.

31. PSPs and IPSPs may demonstrate compliance with the *Wire Transfer Regulations* if they have in place relevant *systems and controls* (including *policies and procedures*) which set out clearly:

- which criteria they use to determine whether or not their services and payment instruments fall under the scope of the *Wire Transfer Regulations*
- which of their services and payment instruments fall within the scope of the *Wire Transfer Regulations* and which do not, and
- which information relating to transfers of funds is required to be recorded, how this information should be recorded, and where.

32. PSPs and IPSPs may demonstrate their compliance with the application of the exemption under Article 2(3) of the *EU Regulation* when they have procedures for identifying and documenting:

- that transfers by card, instrument or device are for goods or services, where the exemption applies, as opposed to person-to-person transfers and
- that their *systems and controls* ensure that the number of the card, instrument, or digital device, for example, the Primary Account Number (PAN), is provided in a way that allows the transfer to be traced back to the payer.

14.1.3 Outgoing transfers – obligations upon the PSP of the payer

14.1.3.1 Transfers for non-account holders

Statutory requirements (paraphrased wording)

33. *Under Article 4(3) EU Regulation, the PSP of the payer shall ensure that transfers of funds are accompanied by the following complete information on the payer and the payee:*

a) the name of the payer;

b) unique transaction identifier (which can trace a transaction back to the payer);

c) one of either the 'payer's address, official personal document number, customer identification number or date and place of birth;

d) the name of the payee; and

e) a unique transaction identifier (which can trace a transaction back to the payee).

34. *These requirements apply to all types of transfers outside the British Islands and exceeding €1,000, whether those transfers are carried out in a single transaction or in several transactions which appear to be linked.*

35. *The 'unique transaction identifier' is defined as a combination of letters, numbers or symbols determined by the PSP, in accordance with the protocols of the payment and settlement systems or messaging systems used for the transfer of funds, which permits the traceability of the transaction back to the payer and the payee.*

36. *The following derogation applies, allowing for a reduced information to be provided:*

- *Under Article 5 of the EU Regulation, where all of the PSPs involved in the payment chain are established in the British Islands, the transfer shall include at least the unique transaction identifier (which can trace a transaction back to the payer and payee) for the payer and the payee. If further information is requested by the PSP of the payee or the Intermediary PSP, such information shall be provided within three working days of the receipt of a request for such information;*
- *Under Article 6, where PSP of the EU Regulation of the payee is established outside the British Islands, transfers of funds not exceeding €1,000 shall be accompanied by at least: the names of the payer and the payee and the unique transaction identifier.*

Note: For transfers of funds not exceeding € 1,000 the PSP of the payer need not verify the information on the payer unless the funds to be transferred have been received in cash or in anonymous electronic money, or the PSP has reasonable grounds for suspecting money laundering or the financing of terrorism.

14.1.3.2 Transfers for Account holders

Statutory requirements (paraphrased wording)

37. *Under Article 4(1) and 4(2), where a transfer of funds is made from or to an account, the PSP of the payer shall ensure that transfers of funds are accompanied by the following complete information:*

a) the name of the payer;

b) the payer's payment account number; and

c) one of either the payer's address, official personal document number, customer identification number or date and place of birth;

d) the name of the payee; and

e) the payee's payment account number

38. *These requirements apply to all types of transfers outside the British Islands and exceeding €1,000, whether those transfers are carried out in a single transaction or in several transactions which appear to be linked.*

39. *Under Article 5 and 6 of the EU Regulations the following derogation from the requirements of Article 4 apply:*

- *where all of the PSPs involved in a transfer are established in the British Islands, Article 5 of the Regulation requires that the transfer includes a payment account number of the payer and the payee. The account number could be but is not required to be, expressed as the IBAN. If further information (for example, the name and address of the payer) is requested by the PSP of the payee or the IPSP, such information shall be provided by the PSP within three working days;*
- *under Article 6, where PSP of the payee is established outside the British Islands, transfers of funds not exceeding €1,000 that do not appear to be linked to other transfers of funds which, together with the transfer in question, exceed €1 000, shall be accompanied by at least: the names of the payer and the payee and the payment account numbers of the payer and of the payee.*

Note: For transfers of funds not exceeding € 1,000 the PSP of the payer need not verify the information on the payer unless the funds to be transferred have been received in cash or in anonymous electronic money, or the PSP has reasonable grounds for suspecting money laundering or the financing of terrorism.

AML/CFT/CPF Codes of Practice

[COP125] In the case of a payer that is a company, a wire transfer must be accompanied by an address at which the company's business is conducted, or at which it may be contacted. In the case of a payer that is a trustee, a wire transfer must be accompanied by the address of the trustee.

Guidance notes

40. Linked transactions are defined as at least those transactions that are sent from the same payment account, or from the same payer to the same payee within a short timeframe, for example, within six months. *PSPs* and *IPSPs* may demonstrate that they are able to detect transfers of funds that appear to be linked where they provide, in their *policies and procedures*, examples of scenarios where transfers are found to be linked which are relevant to their type of business.

41. The exemptions for transfers within the British Islands arises from expediency, not principle, in order to accommodate transfers by domestic systems like BACS which are currently unable to include complete information. Accordingly, where the system used for a transfer within the British Islands has the functionality to carry complete information, it is considered a good practice to include it and thereby reduce the likely incidence of inbound requests from payee PSPs for complete information.

42. The verification requirement set out in the *Wire Transfer Regulations* will be met for an account holding *customer* of a PSP where the payer's identity has already been verified by *CDD measures* and is stored, in accordance with the *Money Laundering Order*.

43. To meet the technical limitations and to manage cases with multiple account holders and different addresses, the PSP of the payer may demonstrate compliance with the *Wire Transfer Regulations* by documenting the priority given to the payer's information in line with law enforcement purposes to trace the payer and for sanctions screening. For example, by de-prioritising titles and full middle names, whilst prioritising the initial of the given name and the full family name and at least the country and the city of address; or for joint accounts holders to provide both names, giving priority to family name over given names.

14.1.3.3 Batch Files – payments either inside or outside of British Islands

Statutory requirements (paraphrased wording)

44. *Under Article 6(1), transfers of funds from a single payer to several payees that are to be sent in batch files containing individual transfers shall carry only the payment account number or the unique transaction identifier of the payer, as well as complete information on the payee, provided that the batch file contains complete information on the payer that is verified for accuracy and complete information on the payee that is fully traceable.*

45. *Where the transfer is at or below the €1,000 threshold it need only include:*

(a) the names of the payer and or payee; and

(b) the payment account numbers of the payer and the payee or a unique transaction identifier if there is no payment account for one or both parties.

14.1.4 Incoming Transfers - Obligation on the PSP of the payee and IPSP

Overview

46. Under the Wire Transfer Regulations, the PSPs of the payee and IPSPs are required to implement a targeted and proportionate risk-based approach to the monitoring of incoming fund transfers. The PSP of the payer holds responsibility for communicating all mandatory wire transfer information, which must be transmitted in the designated data fields of the payment message scheme.

47. If the required information on the payer or the payee has been provided only in part (incomplete information) or has not been provided (missing information), there is an increased threat of *money laundering* or *terrorist financing* presented by anonymous transfers.

48. To address the potential risk presented by such transfers, PSPs of the payee should put in place the following measures, ensuring they are commensurate with and proportionate to the *money laundering* and *terrorist financing* risks to which the PSP or IPSP are exposed:

- effective *systems and controls* to detect transfers of funds that lack required information; and
- risk-based *policies and procedures* to determine whether to execute, reject or suspend a transfer of funds that lacks the required information.

49. Effective *policies and procedures* should be set up in a way that reflects the adoption of a risk-based approach and should clearly document the following aspects:

- which information relating to transfers of funds has to be recorded, how this information should be recorded, and where it is stored;
- which transfers of funds have to be monitored in real time and which transfers of funds can be monitored on an *ex-post* basis, and why;
- the obligations of members of staff where they detect missing or incomplete information and the processes they should follow.

50. PSPs of the payee should document which high-risk factors or combination of high-risk factors are to be considered when determining the risk-based approach, for example:

- residual risks (risk posed by the types of *customers*, products, services, and delivery channels);
- country risks (association with high-risk jurisdictions or relevant sanctions regimes);
- unusual value and volume of transactions (compared to their particular business model);
- a negative *AML/CFT/CPF* compliance record on the part of the PSP of the payer or the prior PSP in the payment chain.

51. PSPs of the payee and IPSPs should implement three methods of wire transfer monitoring: real-time monitoring, post-event monitoring, and random post-event sampling. It should be determined and documented which high-risk factors (or combinations of high-risk factors) will always trigger real-time monitoring, and which will trigger a targeted ex-post review. In cases where ex-post monitoring identifies concerns, subsequent transfers of funds should always be monitored in real time.

52. In addition to real-time and targeted ex-post monitoring, PSPs of the payee and IPSPs should regularly perform ex-post reviews on a random sample taken from all processed transfers of funds.

14.1.4.1 Admissible characters or input and missing information checks

Statutory requirements (paraphrased wording)

53. *Under Article 7(1) and Article 11(1), the PSP of the payee and the IPSP respectively shall implement effective procedures to detect whether the fields relating to the information on the payer and the payee in the messaging or payment and settlement system used to effect the transfer of funds have been filled in using characters or inputs admissible in accordance with the conventions of that system.*

54. *Under Article 7(2) and Article 11(2), the PSP of the payee and the IPSP shall implement effective procedures, including, where appropriate, ex-post monitoring or real-time monitoring, to detect whether the payer or payee information listed in those articles is missing.*

AML/CFT/CPF Codes of Practice

[COP126] A PSP of the payee must subject incoming payment traffic to an appropriate level of post-event risk-based sampling to detect non-compliant transfers.

Guidance notes

55. PSPs of the payee and IPSPs may demonstrate compliance with the *Wire Transfer Regulations* by conducting and documenting a risk assessment that covers their payment activities, taking into account the overall volume and jurisdictions of funds transfers and the roles of all bodies involved.

56. PSPs of the payee and IPSPs may demonstrate compliance with the obligation to detect inadmissible characters and inputs if their system's validation rules adopt certain controlling functions, for example, the automatic prevention of sending/receiving of payments/value with inadmissible characters or inputs.

57. Other specific measures may be considered for a "meaningful character check". For example, in some cases the payer and payee information fields may include incorrect or meaningless information which does not make sense, even if this information has been provided using characters or inputs in accordance with the conventions of the messaging or payment and settlement system, for example, "our client", 'my *customer*'', etc. A *supervised person* may identify these issues by undertaking sample testing, maintaining a list of commonly found meaningless terms and keeping it up to date.

58. In addition to real-time and targeted ex-post monitoring, PSPs of the payee and IPSPs may demonstrate an appropriate level of *systems and controls* where they perform ex-post reviews on a random sample taken from all processed transfers of funds.

59. PSPs of the payee and IPSPs may also wish to consider other specific measures, e.g., checking, at the point of payment delivery, that payer information is compliant and meaningful on all transfers that are collected in cash by payees on a "pay on application and identification" basis.

60. PSPs of the payee and IPSPs may draw on existing *policies and procedures* if they are considered sufficient to meet their obligations under the *Wire Transfer Regulations*, as long as those *policies and procedures* are subject to periodic reviews and updates, and training is provided to all relevant members of staff, including persons responsible for processing transfers of funds.

14.1.5 Managing transfers of funds with missing information or inadmissible characters or inputs

Statutory requirements (paraphrased wording)

61. *Under Article 8(1) and Article 12(1), the PSP of the payee and the IPSP shall implement effective risk-based procedures – including the measure referred to in Article 3(5) of the Money Laundering Order – for determining whether to execute, reject or suspend a transfer of funds lacking the required complete payer and payee information and for taking the appropriate follow-up action.*

62. *Under Article 8(2) and Article 12(2), the PSP of the payee and the IPSP should consider the most appropriate course of action on a risk-sensitive basis, which may initially include the issuing of warnings and setting of deadlines. Where the requested information is not provided by the set deadline, the PSP or IPSP should, in line with its risk-based policies and procedures:*

a) decide whether to execute or reject the transfer;

b) consider whether or not the prior PSP in the payment chain's failure to supply the required information gives rise to suspicion; and

c) consider the future treatment of the prior PSP in the payment chain for AML/CFT compliance purposes e.g. rejecting any future transfers of funds from that PSP, or restricting or terminating its business relationship with that PSP.

63. *Under Article 9, separate from the decision whether to execute, suspend or reject a transaction, missing or incomplete information must be considered as a factor when assessing whether a transfer of funds, or any related transaction, is suspicious and whether a disclosure is to be made under Article 34D(4) of the Proceeds of Crime Law, Articles 21(2) of the Money Laundering Order or Article 21(4) of the Terrorism Law.*

Guidance notes

64. To determine whether to reject, suspend or execute a transfer of funds in compliance with Articles 8 and 12, PSPs of the payee and IPSPs may consider the *money laundering*, *terrorist financing*, or *proliferation financing* risks associated with that transfer of funds and document it, for example:

- what *money laundering*, *terrorist financing,* or *proliferation financing* concerns the type of missing information gives rise to; and
- what high-risk indicators have been identified that may suggest that the transaction presents a high *money laundering*, *terrorist financing,* or *proliferation financing* risk or gives rise to suspicion of *money laundering*, *terrorist financing,* or *proliferation financing*.

65. PSPs of the payee and IPSPs may demonstrate implementation of effective risk-based *policies and procedures* by documenting and recording all of their actions and reasons for their actions or inaction, including:

- making a decision on rejecting the transfer and informing the prior PSP in the payment chain of the reason for the rejection;
- making a decision on execution of the transfer and sending of a request for information, before or after crediting the payee's payment account or making the funds available to the payee;

- all appropriate follow-up steps taken to obtain the response, including the issuing of warnings and setting of deadlines, before either rejecting any future transfers of funds from that prior PSP or restricting or terminating its *business relationship* with that prior PSP.

14.1.5.1 Failure to provide information

66. *Under Article 8(2) and Article 12(2) should the PSP of the payer repeatedly fail to provide the required information on the payer or the payee, even after warnings and deadlines, the PSP of the payee or IPSP shall take further steps by:*

- *either rejecting any future transfers of funds from that PSP; or*
- *restricting or terminating its business relationship with that PSP.*

67. *The PSP of the payee or IPSP shall report that failure, and the steps taken, to the JFSC.*

Guidance notes

68. A range of criteria may be used in order to assess whether a PSP of the payer or IPSP is 'repeatedly failing' to provide information, for example:

- the percentage of transfers with missing information sent by a specific PSP or IPSP within a certain timeframe;
- the percentage of follow-up requests that were left unanswered or were not adequately answered by a certain deadline;
- the level of cooperation of the requested PSP or IPSP relating to previous requests for missing information;
- the type of information which is missing.

69. The report to the *JFSC* should be completed without undue delay and contain the following information as set out in the *JFSC* form at **Appendix E1** of *this Handbook*:

- the name of the PSP of the payer or IPSP identified as repeatedly failing to provide the required information;
- the country in which the PSP of the payer or IPSP is authorised;
- the nature of the breach, including:
  - the frequency of transfers of funds with missing information;
  - the period of time during which the breaches were identified; and
  - any reasons the PSP of the payer or IPSP may have given to justify their repeated failure to provide the required information.
- details of the steps the reporting PSP of the payer or IPSP has taken, including the issuing of warnings or deadlines up until the decision to restrict or terminate the relationship was made.

70. The obligation to report applies only to circumstances where information requests are not fulfilled and the PSP of the payee or IPSP invokes measures which restrict or terminate the *business relationship* with the PSP of the payer. The reporting requirement does not apply where a request for information is fulfilled by the PSP of the payer.

14.1.5.2 Additional obligations on IPSPs

Statutory requirements (paraphrased wording)

71. *Under Article 10, the IPSP shall ensure that all the information received on the payer and the payee that accompanies a transfer of funds is retained with the transfer.*

Guidance notes

72. IPSPs should satisfy themselves that their *systems and controls* enable them to comply with the requirement that all information on the payer and the payee that accompanies a transfer of funds is retained with that transfer. As part of this, IPSPs should satisfy themselves of their system's ability to convert information into a different format without error or omission.

14.1.6 Reporting of breaches

Statutory requirements (paraphrased wording)

73. *Under Article 21(1), PSPs shall notify the JFSC of any breaches of the Wire Transfers Regulations.*

74. *Article 21(2) requires PSPs to establish appropriate internal procedures for their employees, or persons in a comparable position, to report breaches internally through a secure, independent, specific and anonymous channel, proportionate to the nature and size of the PSP.*

75. *Under Regulation 3 of the Wire Transfers Regulations, a relevant person who contravenes any requirement of Article 21(2), shall be guilty of an offence and liable to imprisonment for a term of 2 years and to a fine. This applies to all PSPs and IPSPs, irrespective of the capacity within which the PSP or IPSP is acting.*

Guidance notes

76. A *supervised person* should ensure that any breach of the *Wire Transfer Regulations* is promptly reported to the *JFSC.*

77. The report to the *JFSC* should be completed without undue delay and contain the following information as set out in the form at **Appendix E2** of *this Handbook*:

- the specific provision in the *Wire Transfer Regulations* which has been breached;
- the nature of the breach, including its cause;
- the date the breach was identified by the PSP; and
- where possible, a summary of the measures taken by the PSP in relation to the breach and any subsequent changes to its *systems and controls* (including *policies and procedures*) to mitigate against a recurrence.

78. A *supervised person* should establish *policies and procedures* for the internal reporting of breaches of the *Wire Transfer Regulations* and maintain a record of those breaches and action taken, ensuring sufficient confidentiality and protection for *employees* who report breaches committed within the *supervised person*.

14.1.7 Information, data protection and record retention

Statutory requirements (paraphrased wording)

79. *Under Regulation 3 of the Wire Transfers Regulations, a relevant person who contravenes any requirement of Articles 14, 15(2) or (3), or 16 of the EU Regulation shall be guilty of an offence and liable to imprisonment for a term of 2 years and to a fine. This applies to all PSPs and IPSPs, irrespective of the capacity within which the PSP or IPSP is acting.*

80. *Under Article 14 of the EU Regulation, a relevant person shall respond fully and provide without delay all requested information concerning wire transfers to Jersey authorities responsible for preventing and combating money laundering or terrorist financing.*

81. *Under Article 15(2) of the EU Regulation, personal data shall be processed by PSPs only for the purposes of the prevention of money laundering or terrorist financing and shall not be further processed in a way that is incompatible with those purposes. The processing of personal data for commercial purposes shall be prohibited.*

82. *Under Article 15(3) of the EU Regulation, PSPs shall provide new customers with the information required pursuant to the Data Protection (Jersey) Law 2018 before establishing a business relationship or carrying out an occasional transaction (i.e. a one-off transaction). That information shall, in particular, include a general notice concerning the legal obligations of PSPs under the EU Regulation when processing personal data for the purposes of the prevention of money laundering or the financing of terrorism.*

83. *Article 16 of the EU Regulation requires that information on the payer and the payee shall not be retained for longer than is strictly necessary. PSPs of the payer and of the payee shall retain records of the information referred to in Articles 4 to 7 for a period of six years.*

Guidance notes

84. The "authorities responsible for preventing and combating *money laundering* or *terrorist financing*" described in Article 14 of the *EU Regulations* should be understood in Jersey to be the *JFSC* and the States of Jersey Police, including the *FIU*.

14.1.8 Offences and criminal liability

Statutory requirements (paraphrased wording)

85. *Under Regulation 3 of the Wire Transfers Regulations, a relevant person, whether acting in the capacity of PSP of the payer, PSP of the payee or an IPSP, who contravenes any requirement of the specific provisions of the EU Regulations, which have effect in Jersey by virtue of Regulation 2, shall be guilty of an offence and liable to imprisonment for a term of 2 years, and to a fine as follows:*

- *PSP of the payer - Articles 4, 5, 6 (see section 11.3 Outgoing Transfers - Obligations upon the PSP of the Payer);*
- *PSP of the payee - Articles 7, 8, 9 (see section 11.4 Incoming Transfers - Obligations upon the PSP of the payee and IPSP);*
- *IPSP - Articles 10, 11, 12 (see section 11.4 Incoming Transfers - Obligation upon the PSP of the payee and IPSP).*

86. *In deciding whether a person has committed an offence under the Wire Transfers Regulations, the court shall take into account whether the person followed any relevant guidance that applies to the person, and which was at the time issued, adopted or approved by the JFSC under any other enactment.*

87. *A person shall not be guilty of an offence under the Wire Transfers Regulations if they took all reasonable steps, and exercised all due diligence, to avoid committing the offence.*

88. *Under Regulation 4(1) of the Wire Transfers Regulations, if an offence under these Regulations committed by a limited liability partnership, a separate limited partnership, any other partnership having separate legal personality or a body corporate is proved to have been committed with the consent or connivance of:*

> *(a) a person who is a partner of the partnership, or a director, manager, secretary or other similar officers of the body corporate; or*
>
> *(b) any person purporting to act in any such capacity;*
>
> *the person is also guilty of the offence and liable in the same manner as the partnership or body corporate to the penalty provided for that offence.*

89. *Under Regulation 4(2) of the Wire Transfers Regulations, if the affairs of a body corporate are managed by its members, paragraph (1) applies in relation to acts and defaults of a member in connection with the member's functions of management as if they were a director of the body corporate.*

14.2 Prepaid cards

Overview

90. This section helps *supervised persons* issuing prepaid cards in Jersey (**issuers**), whether directly or indirectly through an agent or a distributor. It covers:

- what electronic money is and the features of prepaid cards;
- the various operators involved in a prepaid card programme;
- examples of risk factors inherently associated with prepaid cards;
- examples of how prepaid cards have been used in Jersey by *money launderers;* and
- the relevant regulatory and supervisory framework in place in Jersey in respect of the provision of prepaid cards.

14.2.1 Electronic money

Overview

91. Electronic money is defined at paragraph 5(d)(15) of the Schedule to the *Wire Transfers Regulations* as "electronically (including magnetically) stored monetary value, as represented by a claim on the issuer, which is issued on receipt of funds for the purpose of making a payment transaction, and which is accepted by a person other than the issuer of the electronic money".

92. Examples of electronic money products and services include online payment services, card-based products (including prepaid cards), vouchers and mobile payment services.

93. Monetary value will be stored in an **online account** or held on a **stored-value card** (where the value is stored on a microchip embedded in the card). Both may be reloadable or non-reloadable. A **reloadable** account or stored-value card can be recharged after the initial funds have been loaded, usually for an unlimited number of times. A **non-reloadable** account or stored-value card can be charged only once and does not permit any other funds to be added.

94. Electronic money which is card-based uses the card for authentication to permit a *customer* to access their funds.

95. Where electronic money is not used it can instead be redeemed. **Redemption** is a process whereby a *customer* presents electronic money to the issuer and receives money in exchange at par value. Redemption should not be confused with the spending of electronic money when a prepaid card is used for purchase of goods or services from merchants.

96. Card-based electronic money may be used in an open or closed loop system. In an **open loop system** card may be used to purchase goods and services from any merchant or withdraw cash at *ATMs* operated by any merchant that is participating in the payment network. These cards provide access to the global *ATM* and payment network through the logo that the card is branded with (e.g., VISA, MasterCard and American Express). In a **closed loop system**, cards may be used only to purchase goods and services from a single merchant or a limited, closed network of merchants (e.g., gift cards, gift vouchers and gift certificates). These cards typically do not provide access to the global *ATM* network, cannot be recharged and have no "cash back" function.

14.2.2 What is a prepaid card?

Overview

97. Prepaid cards are a type of electronic money. The *FATF* has classified such cards as a type of *NPPS*. These are new and innovative payment products and services that offer an alternative to traditional financial services. Other types of *NPPS* include mobile payment services and internet-based payment services – these are not covered by this section.

98. Prepaid cards provide the holder with an authenticated access to pre-loaded funds. These funds can be held in an online account or on a stored-value card.

99. Prepaid cards can be utilised for a range of purposes, including transactions in other countries or territories. Some cards can be funded by cash or other electronic payment instruments and can be used for online shopping or to receive "cash back". Newer prepaid card features that are becoming increasingly common include making onward transfers of money from a prepaid card account to other accounts (known as person-to-person transfers) and setting up standing orders.

100. Prepaid cards are a retail product and are mostly used for making small value payments. Despite this, the range of functions which prepaid cards currently offer can make them attractive to criminals.

14.2.3 Who is involved in a prepaid card programme?

Overview

101. Several operators are normally involved in a prepaid card programme. These include:

Operator	Description
acquirer	The person which maintains the relationship with the retailer, provides the infrastructure needed for accepting a card payment (e.g., access to the point of sale (**POS**) terminal or the payment services supporting an e-commerce website) and normally operates the account in which the proceeds of the sale transaction are deposited.
distributor/ retailer	The person that sells, provides, or arranges for the sale of, prepaid cards on behalf of the issuer to *customers*. Distributors may also offer a separate range of services to these *customers*.
payment network operator	The person that provides the technical platform to perform transactions with the card at *ATMs* or points of sale at merchants.
issuer	The person that issues prepaid cards and against which the *customer* has a claim for redemption or withdrawal of funds.
programme manager	The person responsible for establishing and managing the prepaid card programme in cooperation with a bank or electronic money institution. The programme manager usually markets the prepaid cards and establishes relationships with banks and distributors or *customers*, and in many cases provides the data processing capability. Some prepaid card issuers manage their card programmes themselves (i.e., without using programme managers).
agent	For the purposes of this section of *the Handbook*, the agent is any person that issues prepaid cards on behalf of the issuer (the principal), whether by contract with, or under the direction of, the principal.

102. Article 1 of the *EU Directive* stipulates that the activity of issuing electronic money falls within its scope. Categories of electronic money issuers include:

- credit institutions;
- electronic money institutions (defined in Article 2 of the *EU Directive* as a legal person that has been granted authorisation to issue electronic money); and
- post office giro institutions.

103. An issuer will be considered to carry on a *supervised business* in or from within Jersey where it does so through a physical presence on the island or through a Jersey-based agent.

14.2.4 Risks associated with prepaid cards

Overview

104. The *FATF* issued a guidance paper in June 2013 regarding the application of a risk-based approach towards prepaid cards, mobile payments and internet-based payment services. This paper highlights the importance of taking a more enhanced and focused approach in areas where there are higher risks.

105. Whilst prepaid cards do not automatically present a higher risk of *money laundering*, *terrorist financing,* or *proliferation financing*, issuers will need to consider the specific risk factors of each card issued and determine its risk assessment based on the same. The risk of a prepaid card being misused will also depend on the product design and use and the effectiveness of *systems and controls* (including *policies and procedures*). Issuers are expected to exercise greater caution and **apply *enhanced CDD measures*** in instances where there is a **greater** *money laundering, financing of terrorism,* or *financing of proliferation* **risk** or where a product is designed and used in a way that is similar to a bank account.

106. The risk assessment of a prepaid card issuer will need to cover all relevant risk factors (e.g., *customer* profile, product design and functionalities, geographical location of main card funding and card spending activities).

Guidance notes

107. Prepaid cards are mostly used for making small value payments and transactions. They leave an audit trail in the system, unlike cash transactions. However, if certain risk factors are not adequately or effectively managed and mitigated, prepaid cards can become attractive or susceptible to *money launderers*, *terrorist financiers* or *proliferation financiers* of weapons of mass destruction.

108. The risk factors listed below do not constitute an exhaustive list and should not be considered in isolation. An accumulation of multiple risk factors will increase the overall risk level – such an accumulation is often seen in cases where prepaid cards have been used to facilitate criminal activities.

- Prepaid cards are **portable** and easily transported **cross-border**. The current definition of cash and bearer negotiable instruments in the Customs and Excise (Jersey) Law 1999 does not extend to prepaid cards and there is no requirement to report mailing or shipping such cards abroad. Furthermore, it can be difficult for law enforcement, customs, or border guards to determine and potentially seize the monetary value stored on a prepaid card. This is particularly relevant when prepaid cards have high load limits and are used to transport the proceeds of criminal activities;
- Ownership of the card may be transferred to an **unidentified bearer** (i.e., from the *customer* to another person);
- Prepaid cards may be purchased, and funds loaded, reloaded, redeemed, or withdrawn on a **non-face-to-face basis;**
- Prepaid cards may be **funded by cash** which could be the proceeds of criminal activity. Cards also provide **access to cash** by way of *ATMs*, "**cash back**" functionality or redemption;
- Prepaid cards may **be funded by unidentified third parties** and by other electronic products;
- The card may have a **high transaction limit** or **no transaction limit** at all. Prepaid cards that allow high values to be loaded, have high or no transaction value limits and high or no transaction frequency limits increase the risk of *money laundering,* the *financing of terrorism,* or the *financing of proliferation;*
- Individual *customers* or groups of *customers* may hold, have access to, or control **multiple cards**. Multiple cards can be transported or sent across borders in an attempt to circumvent the usual controls of cross-border cash movements;
- Prepaid cards may be used to make **frequent or high value cross-border transactions** by allowing *customers* to use funds loaded on their cards to be transferred onwards to other persons (person to person or business to business transfers);

- Most prepaid card programmes involve a number of agents which may be based in several different countries and territories. As a result of this segmentation there may be a **lack of consistent *CDD* measures** being applied across the issuer's business;
- Prepaid card operators typically **outsource business and compliance functions** to overseas locations, where the legislation **may not necessarily follow international standards**.

109. **Case study: Use of prepaid cards to launder the proceeds of crime**

- Prepaid currency cards have been used by individuals in Jersey to launder the proceeds of drug trafficking. For example, prosecutions in 2013 were connected with the laundering of criminal proceeds, amounting to £157,000, in Jersey through foreign currency exchange operators and through multiple loadings of criminal funds onto prepaid cards. In the case of the latter method, funds loaded locally were then withdrawn overseas, over a period of 34 months.
- Evidence demonstrated that individuals hired by the drug dealer were asked to "bank" the proceeds of illicit drugs sales by obtaining prepaid cards (two individuals held two cards each in their own names), loading cash onto these prepaid cards in Jersey, and subsequently withdrawing these funds in the UK and Spain.
- This case shows that criminals will exploit the different functionalities offered by prepaid cards. The ability to obtain multiple cards and load them with third party cash, the portability of such cards, and the ability to withdraw cash abroad have proved attractive to criminals.

14.2.5 Regulatory framework – prudential and conduct of business

Overview

110. There is currently no prudential or conduct of business regime in place in Jersey covering prepaid card issuers. However, in certain circumstances it is possible that prepaid card activity may fall within other regulatory regimes established, for example under the *BB(J) Law* (deposit-taking) or the *FS(J) Law* (where funds loaded on to a card are held by a card issuer in a trustee capacity).

14.2.6 Regulatory framework – *AML/CFT/CPF*

Overview

111. The activity of issuing prepaid cards is listed in paragraph 6 of Part 2 of Schedule 2 to the *Proceeds of Crime Law*: "Means of payment" issuing and administering means of payment (such as credit and debit cards, cheques, travellers' cheques, money orders and bankers' drafts, and electronic money)".

112. As a result, any person issuing electronic money (including prepaid cards) in or from within Jersey (directly or through an agent) or through a legal person established under Jersey law:

- becomes a *supervised person* for the purposes of the *Money Laundering Order* and is required to apply *CDD* measures, keep records, appoint an *MLCO* and *MLRO*, and to have *policies and procedures* in place to prevent and detect *money laundering,* the *financing of terrorism,* and the *financing of proliferation*;
- is required to register with the *JFSC* under the *Supervisory Bodies Law* or, where the person carries on a *regulated business* as defined in the *Supervisory Bodies Law*, to notify the *JFSC* that it is issuing prepaid cards; and
- is subject to supervision by the *JFSC* under the *Supervisory Bodies Law* for compliance with the *Money Laundering Order* and *AML/CFT/CPF Codes of Practice*.

113. The *Money Laundering Order* therefore **applies to prepaid card issuers with no physical presence in Jersey** that issue cards through Jersey-based agents.

114. The *Money Laundering Order* does not provide for the application of simplified *identification measures* to prepaid card *customers*. Prepaid card issuers are required to apply *CDD* measures to each *customer* and each third party on whose behalf the *customer* acts.

115. Where a *business relationship* is established with a *customer*, a prepaid card issuer is required to monitor *customer* transactions undertaken throughout the course of that *business relationship*.

116. By virtue of Article 2(3) of the *EU Regulation*, payment cards (among other methods of transfer) are exempt from the scope of the *Wire Transfers Regulations* where they are used exclusively for the purchase of goods or services and the number of the card accompanies all transfers. However, Article 2(3) of the *EU Regulation* also states that the use of a payment card to affect a person-to-person transfer of funds falls within the scope of the *EU Regulation*.

117. This means that where they satisfy the conditions set out in Article 2(3) of the *EU Regulation*, a person carrying on activities listed in paragraph 6 of Part 2 of Schedule 2 to the *Proceeds of Crime Law* is exempt from the obligation to include information on the payer in a wire transfer.