4 GUIDANCE ON PRODUCTS AND SERVICES

4.1 PREPAID CARDS

4.1.1 Overview

1. The purpose of this section is to assist relevant persons issuing prepaid cards (issuers) in Jersey (whether directly or indirectly through an agent or a distributor). It:

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

4.1.2 ELECTRONIC MONEY

2. A definition of **electronic money** in Jersey may be found in Regulation 1 of the Wire Transfer Regulations. Electronic money is monetary value represented by a claim on an issuer that is:

   - stored on an electronic device;
   - issued on receipt of funds of an amount not less in value that the monetary value issued; and
   - accepted as a means of payment by undertakings other than the issuer.

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

4. Monetary value will be stored in an online account or held on a stored-value 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, typically 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.

5. **Card-based electronic money** uses the card for authentication in order to permit a customer to access his or her funds.

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

7. Card-based electronic money may be used in an open or closed loop system. In an **open loop system** cards may be used to purchase goods and services or withdraw cash at ATMs operated by any merchant participating in the payment network. These cards provide access to the global ATM network through the payment network 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.

4.1.3 What is a prepaid card?

8. Prepaid cards are a type of electronic money.

9. According to the FATF, such cards are a type of New Payment Products and Services (NPPS). These are considered to be new and innovative payment products and services that offer an

alternative to traditional financial services. Other types of NPPS (mobile payment services and internet-based payment services) are not covered by this section.

10. At its core, a prepaid card is a card-based product that provides its holder an authenticated access to pre-loaded funds held in an online account on a server or on a microchip embedded in the card (stored-value card).

11. Prepaid cards were introduced in the payments market at the end of the 1990s as an alternative to credit cards and debit cards. Originally developed as a device to pay for goods and services where the issuer did not need to evaluate the card holder's creditworthiness (as required if a credit card was to be issued) nor wish to bear the cost of opening and managing a payment account (in the case of a debit card), prepaid cards nowadays offer a wide range of additional functionalities that can make them attractive to criminals.

12. The multitude of functionalities offered today by prepaid card issuers include payment network branded prepaid cards that can be used internationally, can be funded by cash or other electronic payment instruments, and can be used for online or telephone shopping or to receive "cash back". Increased prepaid card features that resemble debit or credit card functionality include the possibility for onward transfers of money from a prepaid card account to other accounts (so called person-to-person transfers) and the possibility to set up standing orders.

13. Prepaid cards are a retail product that is largely used for making small value payments. Many types of prepaid cards have been developed for different users that offer no or very limited utility for money laundering or financing of terrorism.

4.1.4 Who is involved in a prepaid card programme?

14. A number of operators are typically found in a prepaid card programme.

15. The **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.

16. The **distributor** (including 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.

17. The **payments network operator** – the person that provides the technical platform to perform transactions with the card at ATMs or points of sale at merchants.

18. The **issuer** – the person that issues prepaid cards and against which the customer has a claim for redemption or withdrawal of funds.

19. The **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 also manage their card programmes themselves (i.e. without using programme managers).

20. The **agent** – for the purposes of this section, 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.

21. Article 1 of the Electronic Money Directive stipulates that it is the activity of **issuing** electronic money that falls within the scope of the Directive. Categories of electronic money issuers include: credit institutions; electronic money institutions (defined in Article 2 of the Directive as a legal person that has been granted authorisation to issue electronic money); and post office giro institutions.

22. In Jersey, an issuer will be considered to carry on a financial service business in or from within Jersey where it does so through a physical presence here or through a Jersey-based agent.

4.1.5 What are the risks?

4.1.5.1 FATF guidance

23. The FATF guidance paper for a risk-based approach towards prepaid cards, mobile payments and internet-based payment services (issued in June 2013)[1] highlights the importance of taking a more enhanced and focused approach in areas where there are higher risks.

24. Whilst the extent and nature of measures taken by prepaid card issuers to mitigate money laundering and financing of terrorism risks will vary depending on the level of risk posed by a particular card, issuers are expected to exercise greater caution and apply enhanced measures in instances where there is greater money laundering or financing of terrorism risk or where a product is designed and used in a way that is similar to a bank account.

25. It is important to note, however, that prepaid cards, along with other NPPS in commercial use, do not automatically present a higher risk of money laundering or financing of terrorism. The risk of a prepaid card being used will depend on product design and use and the effectiveness of systems and controls (including policies and procedures).

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

4.1.5.2 Risk factors inherently associated with prepaid cards

27. Prepaid cards are predominantly used for making small value payments and their use leaves an audit trail in the system so that there is not the same level of anonymity as cash transactions. However, if certain risk factors are not adequately or effectively managed and mitigated, prepaid cards may become attractive or susceptible to money launderers and terrorist financiers.

28. The following risk factors should not be treated as exhaustive nor should they be considered and acted upon in isolation. A combination of seemingly unrelated risk factors, e.g. non-face to face relationships, high transaction and load-up limits, issue of multiple cards, and frequent or excessive cash withdrawals, will increase risk and these factors are often seen in cases where prepaid cards have been used to facilitate criminal activities.

29. Prepaid cards are **portable** and easily transported **cross-border**. There is currently no legal requirement to declare cross-border movement of prepaid cards which have a value in excess of €10,000 (or equivalent)[2]. The current definition of cash and bearer negotiable instruments does not extend to prepaid cards and there is no requirement to report mailing or shipping such cards abroad. Furthermore, there is no technology allowing 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 as cash replacement and transport medium to repatriate proceeds of criminal activities.

30. A prepaid card may be used by the holder of such a card (the bearer) rather than the customer: ownership of the card may be transferred to an **unidentified bearer**.

31. Prepaid cards may be purchased, and funds loaded, reloaded, redeemed, or withdrawn on a **non-face-to-face** basis.

32. Prepaid cards may be **funded by cash**, the provenance of which is not easily ascertained, and cards provide **access to cash** by way of ATMs, “cash back” or redemption.

33. Prepaid cards may be **funded by unidentified third parties** and by other electronic products.

34. There may be **high or no transaction limits**. Prepaid cards that allow high loadings, have high transaction and high or no transaction frequency limits increase the risk of money laundering or financing of terrorism.

35. Individual customers may hold, have access to, or control **multiple cards** (an individual holding multiple cards or multiple individuals being linked to one card/electronic account). Given the

[1] FATF Guidance paper

[2] Customs and Excise (Jersey) Law 1999, Article 37A

use of prepaid cards as a cash replacement and transport medium, multiple cards may be physically transported or sent across borders circumventing the control of cross-border movements of cash.

36. Prepaid cards may be used to make **frequent or high value cross-border transactions**. Increased product functionalities allow customers to use funds loaded on their cards to be transferred onwards to other persons (person to person or business to business transfers).

37. Most prepaid card programmes involve a number of agents (some in different countries and territories). As a result of this **segmentation** it may not be possible to apply cohesive CDD measures across the issuer's business.

38. Prepaid card operators typically **outsource business and compliance functions** to overseas locations (where legislation may not follow international standards).

4.1.5.3 Use of prepaid cards to launder the proceeds of criminal activity

39. Prepaid travel (currency) cards have been used by individuals in Jersey to launder the proceeds of drug trafficking. Recent prosecutions have highlighted the laundering of £157,000 of ill-gotten gains 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 withdrawn overseas over a period of 34 months.

40. Evidence shows that individuals "hired" by the drug dealer were asked to "bank" the proceeds of sale of illicit drugs money by obtaining prepaid cards (two individuals held two cards each in their own names), loading cash onto these prepaid cards in Jersey, and withdrawing these funds subsequently in the UK and Spain.

41. This case shows that criminals will exploit the functionalities offered by prepaid cards. The ability to obtain multiple cards and load them with third party cash, portability of such cards, and ability to withdraw cash abroad have proved attractive to perpetrators.

4.1.6 Regulatory and supervisory framework

4.1.6.1 Prudential and conduct of business regulation

42. There is currently no prudential or conduct of business regime in place in Jersey covering prepaid card issuers.

43. In certain circumstances, it is possible that prepaid card activity may fall within the regulatory regimes established under the Banking Business (Jersey) Law 1991 (deposit-taking) or the Financial Services (Jersey) Law 1998 (where funds loaded on to a card are held by a card issuer in a trustee capacity).

4.1.6.2 AML/CFT regulation

44. The activity of issuing prepaid cards is listed in Article 7(1)(e) of Schedule 2 to the Proceeds of Crime Law: issuing and administering means of payment (such as credit and debit cards, cheques, travellers' cheques, money orders and bankers' drafts, and electronic money).

45. 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 relevant 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 and financing of terrorism;
- is required to register with the Commission under the Supervisory Bodies Law or to notify the Commission that it is issuing prepaid cards; and
- is subject to supervision by the Commission under the Supervisory Bodies Law for compliance with the Money Laundering Order and AML/CFT Codes of Practice.

46. Consequently, the Money Laundering Order applies to prepaid card issuers with no physical presence in Jersey that issue cards through Jersey-based agents.

47. The Money Laundering Order does not provide for the application of simplified identification measures to prepaid card customers (e.g. storage, turnover or redemption limits). Prepaid card issuers are required to apply CDD measures to each customer and each third party on whose behalf the customer acts.

48. In a case where a business relationship is established with a customer, a prepaid card issuer is required to monitor transactions undertaken throughout the course of that business relationship with its customer.

49. By virtue of Regulation 5(4) of the Wire Transfer Regulations, a transfer of funds is exempt from the scope of the Wire Transfer Regulations if:

- the transfer is carried out using electronic money;
- the amount transacted is €1,000 or less; and
- the device on which the electronic money is stored:
  - cannot be recharged and the maximum amount stored in the device is no more than €150, or
  - can be recharged and a limit of €2,500 is imposed on the total amount transacted in a calendar year, except if an amount of €1,000 or more is redeemed in that same calendar year by the bearer of the device.

50. This means that, in the circumstances listed in Regulation 5(4) of the Wire Transfer Regulations, a person carrying on activities listed in Paragraph 7(1)(e) of Schedule 2 to the Proceeds of Crime Law is exempt from the obligation to include information on the payer in a wire transfer.

4 GUIDANCE ON PRODUCTS AND SERVICES

4.2 E-ID

4.2.1 Overview

1. The purpose of this section is to assist relevant persons who are considering the use of smart phone and tablet applications to capture information, copy documents and take photographs of customers as part of their CDD processes (referred to hereafter as "**E-ID**"). It:

   - explains the relevant legal and regulatory obligations in relation to CDD;
   - explains the relevant legal and regulatory obligations in relation to new and developing technologies, outsourcing and non-face-to-face customers;
   - highlights risk factors inherently associated with the use of smart phone and tablet applications to capture information, copy documents and take photographs; and
   - provides some examples of risk mitigants to consider when assessing use of a particular smart phone and tablet application.

2. This guidance may also be relevant in situations where similar processes, risks and potential mitigants are present (for example in assessing the risks presented by the use of self-service kiosks with similar document and image capturing and verification technology).

4.2.2 Background

3. In order to properly consider the risks associated with E-ID, it will be necessary for senior management to be very clear about what the smart phone and tablet application does and what it does not do. For example:

   - Is it to be used only to collect information about an individual from that individual?
   - Is it to be used to obtain evidence of that individual's identity?
   - Is it to be used to collect more general relationship information about an individual from that individual, e.g. source of funds?
   - Is it also to be used to collect information about an individual from reliable and independent data sources?

4. To the extent that a smart phone and tablet application does not cover particular elements of identification measures (or more general CDD measures), then, in line with Article 13 of the Money Laundering Order, these should continue to be applied using a relevant person's existing systems and controls (including policies and procedures).

4.2.3 Legal and regulatory obligations in relation to CDD

5. Article 3(4) of the Money Laundering Order explains that identification of a person means:

   - Finding out the identity of that person, including that person's name and legal status; and
   - Obtaining evidence on the basis of documents, data or information from a reliable and independent source, that is reasonably capable of verifying that the person to be identified is who the person is said to be, and satisfies the person responsible for the identification of a person that the evidence does establish that fact.

6. Section 4.3.2 of the AML/CFT Handbook explains how a relevant person may demonstrate that it has obtained evidence that is reasonably capable of verifying that an individual to be identified is who the individual is said to be. Inter alia, it states that use of the following documentary evidence will be reasonably capable of verifying an individual's identity:

   - A current passport, or copy of such a passport certified by a suitable certifier;

- A current national identity card, or copy of such a national identity card certified by a suitable certifier; or
- A current driving licence, or copy of such a driving licence certified by a suitable certifier.

7. As an alternative to using documentary evidence, Section 4.3.4 of the AML/CFT Handbook permits, in certain circumstances, ***the use of independent data sources*** to verify that the person to be identified is who the person is said to be. In practice, it may be possible to demonstrate compliance with Article 3(4) of the Money Laundering Order through a combination of documentary evidence and independent data sources.

8. A relevant person may use other tools and/or methods (including E-ID) to undertake customer due diligence measures, so long as such methods comply with Article 3(4) of the Money Laundering Order.

4.2.4 Legal and regulatory obligations in relation to new and developing technologies, outsourcing and non-face-to-face customers

9. Article 11 of the Money Laundering Order requires a relevant person to have policies and procedures for the identification and assessment of risks that arise in relation to the use of new or developing technologies for new or existing products or services.

10. Article 15(3) of the Money Laundering Order requires a relevant person to apply enhanced CDD measures when the customer has not been physically present for identification purposes.

11. An AML/CFT Code in Section 2.4.4 of the AML/CFT Handbook (and other Handbooks) requires a relevant person to assess, record and monitor risk when any element of the CDD process is outsourced to another party.

12. The Commission considers that all three requirements will apply in any circumstances where a part of the CDD process is undertaken by an independent third party via the use of new technologies where the customer is not present. Accordingly, when deciding whether to make use of a particular smart phone or tablet application, a relevant person is required to:

- Consider the risks involved in the use of the smart phone or tablet application and record the reasons why its use is appropriate.
- Consider the risks involved in outsourcing any part of the CDD process to an independent third party using the smart phone or tablet application and record the reasons why such outsourcing is appropriate.
- Consider whether the features of the smart phone or tablet application work to effectively mitigate the risks identified.
- Apply any additional measures to ensure that all risks are effectively managed.
- Apply on a risk-sensitive basis enhanced CDD measures to take account of the particular risks arising due to the fact that the customer has not been physically present for identification purposes.

13. For the avoidance of doubt, a risk assessment as described in this paragraph is not required to be undertaken on each occasion that the smart phone or tablet application is used, but rather when deciding whether to incorporate the use of the application into CDD measures.

4.2.5 Risks

14. The use of smart phone and tablet applications to apply identification measures presents a number of inherent risks. Typically, an application may do one or more of the following:

- capture information, copy documents and take a photograph of the customer (for instance by way of a camera on a smart phone or tablet);
- transmit the information, documents or photograph (either to the relevant person or another party);
- compare the information, documents and photograph captured;

- verify the information or documents against external data sources.

15. A relevant person may demonstrate that it has considered the particular risks that arise when using smart phone and tablet applications to copy documents and take photographs for CDD purposes when it considers the risks set out at sections 4.2.5.1 to 4.2.5.3.

4.2.5.1 The risk that identification documents are tampered with or forged

16. When original documents are not physically presented, it is more difficult for a relevant person to detect that documents have been tampered with or forged. For example, it may be difficult to detect that a photograph has been inserted into a passport, when simply viewing an electronic copy of the passport.

17. Similarly, it may be difficult to detect the presence or absence of watermarks or other security features on an identity document when simply viewing an electronic copy of the document.

4.2.5.2 The risk that captured copies of documents or photographs are tampered with before or during transmission

18. When an electronic copy of a document has been captured or photograph has been taken, there may be opportunities for the customer (or another party) to use software to alter the copy of the document or photograph before transmitting from the smart phone or tablet. For example, when a customer is merely transmitting a scanned copy of a passport, it may be possible to alter details (such as name, date of birth) on the copy of the passport prior to transmission.

19. Similarly, it may be possible to alter the biometric data (such as a photograph) on a copy of an identity document.

4.2.5.3 The risk that documents presented are stolen or their use unauthorised

20. When a customer is not physically presenting identification documents, it is more difficult for a relevant person to detect that the documents do not belong to the customer. For example, a customer may present stolen documentation.

4.2.6 Considerations for assessing applications

21. This section lists some potential features of smart phone and tablet applications (and wrap-around systems) that may be used to mitigate the risks listed at Section 4.2.5. Where the smart phone or tablet application (or connected system) does not sufficiently mitigate the risk, the relevant person will need to ensure that its CDD systems and controls include measures specifically designed to do so.

22. The list of features below is not exhaustive and other features or systems and controls may be appropriate.

4.2.6.1 Risk that identification documents are tampered with or forged

23. Features of smart phone and tablet applications (and wrap-around systems) that may be used to mitigate the risk that documents have been tampered with or forged may include:

- The copy of the document is of a very high level of clarity and resolution, such that its contents can be adequately viewed and/or enlarged to aid review;
- The copy of the document is automatically matched to a "template' for the particular form of identity document used;
- Data on the document is compared to biometric and other data stored on the machine readable code/algorithm on the document;
- Data on the document is automatically examined for use of unauthorised print fonts and unexpected character spacing;

- The copy of the document is automatically examined to confirm the existence of security features (e.g. watermarks, holograms, micro-text, etc.);
- The copy of the document is examined by individual(s) specifically trained to detect tampering/forgery (e.g. ex-border agents).

4.2.6.2 Risk that captured documents or photographs are tampered with before or during transmission

24. Features of smart phone and tablet applications (and wrap-around systems) that may be used to mitigate the risk that a copy of a document or photograph has been tampered with may include:

- The smart phone or tablet application itself controls the copying of the document, photography, and transmission process, allowing no opportunity to tamper with, or manipulate, documents or photographs. (Compared to, for instance, a prospective customer taking a photograph of a document and transmitting the pdf by e-mail);
- A highly secure connection is used to transmit copies of documents and photographs;
- Application security is regularly tested in order to guard against hacking or other security breaches.

4.2.6.3 Risk that documents presented are stolen or their use unauthorised

25. Features of smart phone and tablet applications (and wrap-around systems) that may be used to mitigate the risk that documents presented are stolen (or their use unauthorised) may include:

- A "selfie" photograph of the customer is taken and biometrically compared/matched to the photograph on the identity document presented - to verify that they relate to the same person;
- A video or "stream" of photographs is taken in order to identify facial movements - to confirm that the customer is present at the time that the photograph is taken - to avoid a photograph being taken of a photograph which may have been stolen or use of which is unauthorised;
- A code or password is sent to the customer who, immediately before the application of E-ID, is photographed while displaying the code or password - to confirm that the customer is present at the time that the photograph is taken - to avoid a photograph being taken of a photograph which may have been stolen or use of which is unauthorised;
- Use of a location match – where the application determines that information and copies of documents are captured and photographs taken at a location that is consistent with the customer's place (or country) of residence.

4.2.6.4 Record-keeping

26. Where a relevant person uses smart phone or tablet applications to capture information, copy documents and take photographs of customers as part of their CDD processes, adequate records must be kept in line with record-keeping requirements in Part 4 of the Money Laundering Order.