3: Electronic money

The purpose of this sectoral guidance is to provide clarification to electronic money issuers on customer due diligence and related measures required by law. As AML/CTF guidance, this sectoral guidance is incomplete on its own and must be read in conjunction with the main guidance set out in Part I and the specialist guidance set out in Part III.

This guidance may be used by all electronic money issuers (as defined in Regulation 2(1) of the Electronic Money Regulations 2011), including authorised electronic money institutions, registered small electronic money institutions, and credit institutions with a Part IV permission under the Financial Services and Markets Act 2000 to issue electronic money. It may also be relevant for EEA authorised electronic money issuers who distribute their ~~priductsproducts~~ products in the UK.

Introduction

What is electronic money?

3.1. Under the Electronic Money Regulations 2011 (Reg. 2(1)), electronic money is defined as:

> *'electronically (including magnetically) stored monetary value as represented by a claim on the electronic money issuer which—*
>
> *(a) is issued on receipt of funds for the purpose of making payment transactions;*
>
> *(b) is accepted by a person other than the electronic money issuer; and*
>
> *(c) is not excluded by regulation 3.'*

3.2. Regulation 3 of the Electronic Money Regulations 2011 states that electronic money does not include:

> *'(a) monetary value stored on instruments that can be used to acquire goods or services only—*
>
> *(i) in or on the electronic money issuer's premises; or*
>
> *(ii) under a commercial agreement with the electronic money issuer, either within a limited ~~—~~network of service providers or for a limited range of goods or services;*
>
> *(b) monetary value that is used to make payment transactions executed by means of any telecommunication, digital or IT device, where the goods or services purchased are delivered to and are to be used through a telecommunication, digital or IT device, provided that the telecommunication, digital or IT operator does not act only as an intermediary between the payment service user and the supplier of the goods and services.'*

3.3. Electronic money is therefore a prepaid means of payment that can be used to make payments to multiple persons, where the persons are distinct legal or natural entities. It may be a card-based, voucher-based, mobile app-based or an online account-based product.

3.4. The Electronic Money Regulations 2011 also provide for a number of exemptions (see para~~graph~~. 3.2 above). Where such products are exempted from financial services regulation, they are also likely to fall outside of the scope of the AML and CTF regulation. Issuers must, however, examine such products on a case-by-case basis to identify whether such regulation continues to apply.

3.5. Electronic money may be issued by banks or building societies with the requisite variation of permission from the FCA, or it may be issued by specialist electronic money institutions, who obtain an authorisation from the FCA under the Electronic Money Regulations 2011 (for other persons also permitted to issue electronic money, such as local authorites, see Regulation 2(1) of the Electronic Money Regulations 2011.) Where electronic money institutions meet the conditions set out in Regulation 13 of the Electronic Money Regulations 2011, they may register with the FCA as small electronic money institutions.

3.6. All issuers of electronic money are subject to the Money Laundering Regulations ~~2007, section 21 A of~~2017, the Terrorism Act 2000, the ~~EC~~ Anti-terrorism, Crime and Security Act 2001, the Wire Transfer Regulation, Schedule 7 to the Counter-terrorism Act 2008 and the Proceeds of Crime Act 2002. They must also comply with the legislation implementing the UK's financial sanctions regime. Issuers of electronic money that are FSMA-authorised persons (i.e. banks and building societies) must also comply with relevant provisions in the FCA's handbook~~.~~ for AML/CTF purposes.

3.7. Electronic money may also be issued into the UK by EEA credit and financial institutions holding the appropriate passport from their home state competent authority under Art. 25 or 28 of the Banking Consolidation Directive (2006/48/EC)~~,~~ or Art~~. 25~~s. 28 and 29 of the Payment Services Directive (~~2007/64/EC~~)EU) 2015/2366 by virtue of Art. 3(1) of the Electronic Money Directive (2009/110/EC). Where such issuance, distribution or redemption is on a cross-border services basis, i.e. without an establishment in the UK, the issuer's AML procedures are regulated by the home state authorities, but issuers must be aware that in some cases, UK legislation may extend to such providers of services. UK AML/CTF legislation will apply where the service is provided through an establishment in the UK.

Definitions

3.8. The following terms are used in this guidance:

- **Card-based products:**

  These are products that employ a card for authentication. The electronic money will usually reside in an account on a server and not on the card itself.

- ~~**Complete information on the payer (CIP)**~~

  ~~For the purposes of the Wire Transfer Regulation, CIP consists of the payer's name, address and account number. The address may be substituted with the payer's date and place of birth, his customer identification number or his national identity number. The account number may be substituted with a unique identifier. See Part III, Specialist guidance 1: *Transparency in electronic payments (Wire transfers)*, paragraph 1.13 for details.~~

- **Electronic Money Association (EMA):**

  The EMA is the EU trade body representing electronic money issuers and alternative payment service providers.

- **Merchant:**

  For the purposes of this guidance, a merchant is a natural or legal person that uses electronic money to transact in the course of business. Where an electronic money issuer is part of a four-party scheme, the issuer might not have a direct business relationship with all merchants.

- **Mobile app-based products:**

  These products provide access to account-based e-money which will usually reside on a remote server.

- **Online account-based products:**

  These are products where the value held by a customer is held centrally on a server under the control of the issuer. Customers access their purses remotely.

- **Payment Service Provider (PSP):**

  ~~A PSP is~~PSPs are defined in Article ~~2~~3(5) of the Wire Transfer Regulation as ~~"a natural or legal person whose business includes the provision~~being inclusive of credit institutions, e-money institutions (full and small) and payment institutions (full and small) that provide transfer of funds services.~~"~~

- **Purse:**

  An electronic money purse is a store of electronic money, usually in the form of an account.

- **Redemption**:

  This is the process whereby a customer presents electronic money to the issuer and receives its monetary value in exchange at par. (Note that the term is also sometimes used in the gift card industry to indicate the spending of value with merchants. This meaning is not intended here.)

- **Three- and four-party schemes:**

  An electronic money system can comprise a single issuer that contracts with both consumer and merchant, or it can be made up of a number of issuers and acquirers, each issuer having its own consumer base, each acquirer its own merchant base. The former is referred to as a three-party scheme, comprising issuer, consumer and merchant, whereas the latter is known as a four-party scheme, comprising issuer, acquirer, consumer and merchant.

- **Voucher~~-~~ based products:**

  Some electronic money products are issued as electronic vouchers of a fixed value that can only be spent once. Any value that remains on the voucher can either be redeemed, or a new voucher issued. The value associated with a voucher is usually held centrally on a server.

- **Wire Transfer Regulation ~~[also known as the Payer~~ (WTR):**

- ~~]:~~ Regulation

  ~~Regulation (EC) 1781/2006~~ (EU) 2015/847 on information ~~on the payer~~ accompanying transfers of funds implements ~~Special~~ FATF Recommendation ~~VII~~16 on wire transfers in ~~EU~~EEA member states. This guidance refers to it as the Wire Transfer Regulation, although this term has no formal standing. ~~Supervision and enforcement provisions for this Regulation are implemented in the UK through the Transfer of Funds (Information on the Payer) Regulations 2007 (SI 2007/3298).~~

Notes

3.9. The ~~annual~~ cumulative turnover limit of an electronic money purse is interpreted as the total amount of electronic money received by a purse during a period of time, whether through the purchase of electronic money~~,~~ or the receipt of electronic money from other persons. ~~'Annual' refers to 12-month periods from the opening of the purse.~~

~~3.10. An approximate Sterling figure has been given for all Euro figures.~~

Money laundering and terrorist financing risks related to electronic money

~~3.11.~~3.10. Electronic money is a retail payment product that is used predominantly for making small value payments. It is susceptible to the same risks of money laundering and terrorist financing as other retail payment products. In the absence of AML systems and controls, there is a significant risk of money laundering taking place. The implementation of AML systems and controls and certain product design features can contribute to mitigating this risk.

~~3.12.~~3.11. Furthermore, where electronic money is limited to small value payments, its use is less attractive to would-be launderers. For terrorist financing and other financial crime, electronic money offers a more accountable, and therefore less attractive means of transferring money compared to cash.

~~3.13.~~3.12. The electronic money products in commercial use today do not provide the privacy or anonymity of cash, nor its utility. This is due to a number of factors. Products may, for example, be funded by payments from bank accounts or credit cards and therefore reveal the identity of the customer at the outset. The use of most electronic money products leaves an electronic trail that can help locate, if not identify, the user of a particular product.

~~3.14.~~3.13. As issuers of electronic money usually occupy the position of intermediaries in the payment process, situated between two financial or credit institutions, they are often able to provide additional transaction information to law enforcement that complements identity data provided by other financial institutions. This may be equally or more valuable evidence than a repetition of the verification of identity process.

~~3.15.~~3.14. Fraud prevention and consumer protection concerns lead to the placement of transaction, turnover and purse limits on products, limiting the risk to both issuer and consumer. These limits act to restrict the usefulness of the product for money laundering, and make unusual transactions more detectable.

3.15. A non-exhaustive list of risk factors that may apply to electronic money products is given in para~~graph.~~ 3.~~19~~18 below; risk mitigating factors are listed in para~~graph.~~ 3.~~21~~20 below. ~~Issuers should in particular be alert to emerging information on financial crime risks specific to electronic money, such as those highlighted by typology reports from the EMA and the FATF, and update their risk assessment processes accordingly.~~ Other risks set out in the draft Risk Factors Guidelines of the Joint Committee of the European Supervisory Authorities and in Part I, Annex 4-II of this guidance also affect issuers ~~(e.g., customer profile or geographical location of activity, see Part I, chapter 4 for details)~~, and issuers should consider these as part of the risk assessment that they undertake. ~~Risk assessment should be an ongoing process and take into account information from~~Issuers should in particular be alert to emerging information on financial crime risks specific to electronic money, such as those highlighted by

~~3.16.~~• Their own transaction monitoring ~~systems.~~ processes;

- The FCA;
- The NCA;
- National and supra-national risk assessments and associated recommendations;
- The Joint Committee of the European Supervisory Authorities;
- The European Commission (EC list of high-risk third countries); and
- Typology reports, such as those from the EMA and the FATF.

~~3.17.~~3.16. The overall ML/TF risk posed by an electronic money product is a function of its design, its use, and the issuer's AML/CTF controls. The overall risk posed is the outcome of competing factors, not any single feature of the product.[1]

[1] The draft Risk Factors Guidelines of the Joint Committee of the European Supervisory Authorities, paras. 31-32, state: "Firms should take a holistic view of the ML/TF risk factors they have identified that, together, will

~~3.18.~~3.17. Issuers will need to put in place risk management processes appropriate to the size and nature of their business and must evidence that they deploy an adequate range of controls to mitigate the ML/TF risks they encounter.

Risk factors

~~3.19.~~3.18. The following factors will increase the risk of electronic money products being used for money laundering or terrorist financing (for ways in which this risk can be mitigated by applying controls or by other means, see para~~graph.~~ 3.21 below):

- High, or no transaction or purse limits. The higher the value and frequency of transactions, and the higher the purse limit, the greater the risk, particularly where customers are permitted to hold multiple purses; the €15,000 ~~[£12,500]~~ threshold for occasional transactions provided in the Money Laundering Regulations ~~2007~~2017 may in this context provide a convenient comparator when assessing such risk;
- Frequent cross-border transactions, unless within a single scheme, can give rise to difficulties with information sharing. Dependence on counterparty systems increases the risk;
- Some merchant activity, such as betting and gaming, poses a higher risk of money laundering. This is because of the higher amounts of funds that are transacted and because of the opportunities presented within the merchant environment;
- Funding of purses by unverified parties presents a higher risk of money laundering, whether it is the customer who is unverified or a third party;
- Funding of purses using cash offers little or no audit trail of the source of the funds and hence presents a higher risk of money laundering;
- Funding of purses using electronic money products that have not been verified may present a higher risk of money laundering;
- The non-~~-~~face-to-face nature of many products gives rise to increased risk~~[2]~~;
- The ability of consumers to hold multiple purses (for example open multiple accounts or purchase a number of cards) without verification of identity increases the risk;
- Cash access, for example by way of ATMs, as well as an allowance for the payment of refunds in cash for purchases made using electronic money, will increase the risk;
- Increased product functionality may in some instances give rise to higher risk of money laundering (product functionality includes person-to-business, person-to-person, and business-to-business transfers);
- Products that feature multiple cards linked to the same account increase the utility provided to the user, but may also increase the risk of money laundering, particularly where the customer is able to pass on linked 'partner' cards to anonymous third parties;

---

determine the level of money laundering and terrorist financing risk associated with a business relationship or occasional transaction. As part of this assessment, firms may decide to weigh factors differently depending on their relative importance."

~~[2] While FATF Recommendation 8 recognises that non face to face business increases risks like identity fraud, impersonation fraud or the use of the product by third parties for illicit purposes, the FATF have recently commented that this does not automatically give rise to a high risk scenario in the sense of FATF Recommendation 5 and therefore does not preclude firms from applying simplified due diligence measures (see FATF report *Money Laundering Using New Payment Methods*, October 2010).~~

- Segmentation of the business value chain, including use of multiple agents and outsourcing, in particular to overseas locations, may give rise to a higher risk;
- The technology adopted by the product may give rise to specific risks that should be assessed.

~~3.20.~~3.19. Absence of any of the above factors will decrease the risk.

Risk mitigating factors

~~3.21.~~3.20. Electronic money issuers address the risks that are inherent in payments in a similar manner to other retail payment products by putting in place systems and controls that prevent money laundering and terrorist financing by detecting unusual transactions and predetermined patterns of activity.

~~3.22.~~3.21. The systems and controls issuers put in place must be commensurate to the money laundering and terrorist financing risk they are exposed to. The detail of issuers' systems and controls will therefore vary. Examples include those that:

- Place limits on purse storage values, cumulative turnover or amounts transacted;
- Can detect money laundering transaction patterns, including those described in the EMA or similar typologies documents;
- Will detect anomalies to normal transaction patterns;
- Can identify multiple purses held by a single individual or group of individuals, such as the holding of multiple accounts or the 'stockpiling' of pre-paid cards;
- Can look for indicators of accounts being opened with different issuers as well as attempts to pool funds from different sources;
- Can identify discrepancies between submitted and detected information, for example, between country of origin submitted information and the electronically-detected IP address, geo-location information or device-related information;
- Deploy sufficient resources to address money laundering risks, including, where necessary, specialist expertise for the detection of suspicious activity;
- Allow collaboration with merchants that accept electronic money to identify and prevent suspicious activity;
- Restrict funding of electronic money products to funds drawn on accounts held at credit and financial institutions in the UK, the EU or a comparable jurisdiction, and allow redemption of electronic money only into accounts held at such institutions.

Customer Due Diligence

~~3.23.~~3.22. The Money Laundering Regulations ~~2007~~2017 require firms to apply customer due diligence measures on a risk-sensitive basis. Customer due diligence measures comprise the identification and verfication of the customer's (and, where applicable, the beneficial owner's) identity and obtaining information on the purpose and intended nature of the business relationship~~.~~ or transaction. There is also a requirement for the ongoing monitoring of the business relationship. Part I, Chapter 5 sets out how firms can meet these requirements.

~~3.24.~~3.23. Detailed guidance for verifying the identity of customers who do not have access to a bank account, or who lack credit or financial history, is provided under the financial exclusion provisions of Part I, ~~paragraphs~~paras. 5.3.~~88~~108 to 5.3.~~105.~~125.

~~3.25.~~3.24. Issuers will also need to satisfy themselves that they comply with sanctions legislation. Guidance on this is provided throughout Part I and in Part I~~, paragraphs 5.3.42 to 5.3.50, and Part I~~II, section 4.

Verification of identity – consumers

~~3.26.~~3.25. Taking account of the risk mitigation features applied to electronic money systems, the approach to undertaking customer due diligence in the electronic money sector is predicated on the need to minimise barriers to take-up of the products, whilst addressing the risk of money laundering and meeting the obligations set out in the Money Laundering Regulations ~~2007.~~2017.

3.26. In addition to normal customer due diligence, the Money Laundering Regulations ~~2007~~2017 specify ~~circumstances where simplified due diligence can be applied. Simplified due diligence is~~ the following exemptions and allowances in relation to customer due diligence:

~~3.27.~~ **The e-money-specific exemption**: Circumstances where an exemption ~~for certain products~~ from the requirement to apply customer due diligence measures~~. There is no exemption from the requirement to monitor the business relationship on an ongoing basis.~~

- ~~—~~ may be applied. A purse must meet specific functionality, storage, turnover and redemption ~~limits~~ restrictions in order to qualify for ~~simplified due diligence~~the e-money-specific exemption (see ~~paragraphs~~paras. 3.30 to 3.~~37~~34 below), and issuers must have systems and controls in place to make sure these ~~limits~~restrictions are not breached. ~~The limits mitigate the risk arising from the non-identification of the customer, with the annual redemption limit reducing the risk by allowing funds to enter the system, but only allowing a relatively small amount (€1,000 [£800]) to exit without verification.~~

- **Simplified due diligence**: Circumstances where simplified due diligence may be applied. The allowance to apply simplified due diligence is risk-based, and where the product is no longer low risk, where the issuer doubts the veracity or accuracy of documents or information previously obtained, or where the issuer suspects money laundering or terrorist financing, customer due diligence and, where appropriate, enhanced due diligence measures must be applied.

3.27. Monitoring of the business relationship and transactions must be undertaken during the application of both the e-money-specific exemption and simplified due diligence. Issuers should also comply with the requirements set out ~~paragraphs~~in paras. 3.~~38~~46 to 3.~~42~~49 below ~~if they want to benefit from the simplified due diligence provisions. Where the product no longer qualifies for simplified due diligence, or the issuer knows, suspects, or has reasonable grounds to suspect money laundering or terrorist financing, customer due diligence and, where appropriate, enhanced due diligence measures must be applied.~~ .

~~3.28. Above the simplified due diligence limits, verification of identity using funding instruments may be undertaken where the overall risk posed by the product is low (see paragraphs 3.44 to 3.50 below). In all other cases, normal customer due diligence must be applied.~~

3.28. Issuers, in common with other financial services providers, are required to verify identity of the customer at the outset of a business relationship. The e-money-specific exemption and simplified due diligence enable issuers to postpone the verification of identity until the exemption limits have been reached. Issuers of electronic money products making use of these provisions should have in place systems to anticipate when a customer approaches the exemption limits. Where there is an obligation to undertake customer due diligence and this cannot be discharged, issuers must freeze the account pending the provision of the required information.

3.29. Enhanced due diligence is required in circumstances giving rise to an overall higher risk. The extent of enhanced due diligence measures required will depend on the level of risk a situation presents (see ~~paragraphs~~paras. 3.~~51~~50 to 3.~~54~~53 below).

The e-money-specific exemption

~~*Simplified due diligence*~~

3.30. The Money Laundering Regulations ~~2007~~2017 (Reg. ~~13(7)(d)) distinguish between~~ 37(1) and (2)) set limits for reloadable and non-reloadable electronic money products ~~and set different limits for simplified due diligence~~, above which customer due diligence measures must be applied:

> ~~*'electronic money, within the meaning of Article 2(2) of the electronic money directive, where: —*~~
>
> ~~*(i) if the device cannot be recharged,*~~ *(1) Subject to paragraph (3), a relevant person is not required to apply customer due diligence measures in relation to electronic money, and regulations 27, 28 and 30 do not apply provided that—*
>
> *(a) the maximum amount which can be stored ~~in~~ electronically is 250 euros or (if the ~~device is no more than 250 euro or, in the case of electronic money~~ amount stored can only be used ~~to carry out payment transactions~~ within the United Kingdom, 500 euro~~; or~~ s;*
>
> ~~*(ii) if the device can be recharged, a limit of 2,500 euro is imposed on the total amount transacted in a calendar year, except when an amount of 1,000 euro or more is redeemed in that same calendar year by the electronic money holder (within the meaning of Article 11 of the electronic money directive).'*~~
>
> *(b) the payment instrument used in connection with the electronic money ("the relevant payment instrument") is—*
>
> *i) not reloadable, or*
>
> *ii) is subject to a maximum limit on monthly payment transactions of 250 euros which can only be used within the United Kingdom;*
>
> *(c) the relevant payment instrument is used exclusively to purchase goods or services;*
>
> *(d) electronic money cannot be added to the relevant payment instrument unless the source of that money is known.*
>
> *(2) Paragraph (1) does not apply to any transaction which consists of the redemption in cash, or a cash withdrawal, of the monetary value of the electronic money, where the amount redeemed exceeds 100 euros.*

Non-reloadable purses

3.31. Electronic money purses that cannot be recharged~~, and whose total~~ may benefit from the e-money-specific exemption if:

- ~~3.31.•~~ The purse limit ~~does not exceed~~ is restricted to €250 ~~[£200]~~ (or €500 ~~[£400] for payment transactions~~ if the amount stored can only be used within the United Kingdom~~, benefit from simplified due diligence.~~);
- The instrument is used only for purchase transactions of goods and services;
- The device cannot be funded with anonymous e-money; and

- The customer does not seek to redeem more than €100 in a single transaction.

3.32. Non-reloadable purses are often sold as gift cards. The purchase of multiple such products is sometimes expected, particularly during certain times of the year~~. Provided that the gift card does not allow for cash access,~~, and the risk of money laundering arising from multiple purchases is likely to remain low. Issuers should, however, adopt a maximum total value that they will allow single customers to purchase without carrying out customer due diligence measures. This total value can be determined on a risk weighted basis, but should not exceed €~~2,500 [£2,200].~~1,000.

Reloadable purses

~~3.33. Electronic money purses that can be rechargedare required to apply customer due diligence measures only when the annual turnover limit of €2,500 [£2,200] is exceeded, or if the customer seeks to redeem the €1,000 [£800] annual allowance or more.~~

~~3.34. Where purses can both send and receive payments, such as, for example, in online account-based products that enable person-to-person payments, the €2,500 [£2,200] turnover limit is applied separately to sending and receiving transactions. In other words, the turnover limit is calculated separately for crediting and debiting transactions, and the verification requirement applied when either of the two is reached.~~

~~3.35. Additionally, and in order to address obligations arising from the Wire Transfer Regulation, issuers must verify the identity of customers seeking to undertake any single sending transaction that exceeds €1,000 [£800] in value, where verification has not already been undertaken (see paragraphs 3.62 to 66 below).~~

~~3.36. Issuers, in common with other financial services providers, are required to verify identity of the customer at the outset of a business relationship. Simplified due diligence enables issuers to postpone the verification of identity until the exemption limits have been reached/exceeded. Issuers of electronic money products benefitting from simplified due diligence should have in place systems to anticipate when a customer approaches the exemption limits. Where there is an obligation to undertake customer due diligence and this cannot be discharged, issuers must freeze the account pending the provision of the required information.~~

~~3.37. In summary, where purses qualify for simplified due diligence, customer due diligence measures must be applied to customers and, where appropriate, beneficial owners, before they:~~

- ~~Exceed the cumulative annual turnover limit of €2,500 [£2,200]; or~~
- ~~Reach the annual redemption limit of €1,000 [£800]; or~~
- ~~Seek to undertake a single sending (debit) electronic money transaction which exceeds €1,000 [£800]; or~~

3.33. ~~Where the issuer suspects money laundering or terrorist financing.~~Electronic money purses that can be recharged may benefit from the e-money specific exemption if:

- The purse limit is restricted to €500;
- The monthly turnover is restricted to €250;
- The instrument is restricted to use within the United Kingdom;
- The instrument is used only for purchases of goods and services;
- The device cannot be funded with anonymous e-money; and
- The customer does not seek to redeem more than €100 in a single transaction.

Simplified due diligence

3.34. Issuers may apply simplified due diligence measures in addition to the limits set by the e-money-specific exemption if business relationships or transactions present a low risk of money laundering or terrorist financing.

3.35. Simplified due diligence must always involve the identification and verification of the customer, but the extent of identification and verification can be varied depending on the risk, and verification may be postponed[3] until the risk is no longer deemed to be low. In this case, issuers should set a reasonable threshold that will minimise potential abuse of the product.

3.36. Simplified due diligence may also involve verifying identity on the basis of fewer or less reliable sources, using alternative methods to verify identity, assuming the nature and intended purpose of the business relationship where this is obvious or reducing the intensity of monitoring.

Verification by reliance on the funding instrument under simplified due diligence

3.37. As part of a risk-based approach to verification of identity, the Money Laundering Regulations 2017 require that verification is carried out "on the basis of documents or information obtained from a reliable source which is independent of the customer." In some cases, where the risk associated with the business relationship is low, a customer's funding instrument (such as a credit card or bank account) can constitute such information, subject to the following additional requirements:

a) The issuer remains ultimately responsible for meeting its customer due diligence obligations;

b) The issuer has in place systems and processes for identifying incidents of fraudulent use of credit/debit cards and bank accounts;

c) The issuer has in place systems and processes that enable monitoring to identify increased risk for such products, even within the permitted turnover limits. If the risk profile can then no longer be regarded as low risk, additional verification steps must be undertaken;

d) The issuer records and keeps records of relevant information, for example IP addresses, which assist in determining the electronic footprint of the customer, or where a POS terminal is used in a face-to-face environment, records the correct use of a PIN or other data;

e) The funds to purchase electronic money are drawn from an account or credit card with, or issued by, a credit or financial institution[4] in the UK, the EU or an equivalent jurisdiction, which is supervised for its AML controls;

f) The issuer implements systems and controls to mitigate the risk of the funding card or account being itself subject to SDD;

g) The issuer has reasonable evidence to conclude that the customer is the rightful holder of the account on which the funds are drawn (which may be achieved using the processes described in para. 3.41 below);

h) The overall amount transacted by one customer does not exceed a maximum turnover limit of €15,000 from the commencement of the business relationship.

[3] See the draft Risk Factors Guidelines of the Joint Committee of the European Supervisory Authorities, paragraph 124. Also see Part I, Annex 5-III.

[4] Other than a money service business, or a payment or electronic money institution providing mainly money remittance services.

3.38. Where the above are not satisfied, further customer due diligence measures have to be applied.

3.39. A funding instrument on its own, however, is a weak form of verification of identity. The credit or financial institution whose evidence is being used may not have verified the customer to current standards, and there is a risk that the person using the account is not its rightful holder. This risk is even higher where an electronic money issuer has no evidence that the account is held in the same name as the customer, as is the case, for example, in relation to direct debits.

Establishing control over the funding instrument

3.40. Where payment is made electronically, it is usually not possible to verify the name of the account holder for the funding account. In this case, steps must be taken to establish that the customer is the rightful holder of the account from which the funds are drawn. These steps may include the following:

- Micro-deposit. Some issuers have developed a means of establishing control over a funding account using a process that is convenient and effective. A small random amount of money is credited to a customer's funding account and the customer is then required to discover the amount and to enter it on the issuer's website. By entering the correct value, the customer demonstrates access to the bank/card statement or accounting system of their bank or financial institution. This method, and its close variants (such as the use of unique reference numbers), provides an acceptable means of confirming that the customer has access to the account, and therefore has control over it. It also provides a means of guarding against identity theft, contributing therefore to the verification of identity process. If such an approach is not used, some other means of establishing control of the account is needed.
- Additional fraud checks. Issuers may also use additional fraud checks undertaken at the time of the transaction which seek to cross reference customer-submitted data against data held by the electronic money or card issuer or similar independent third party, and which gives the electronic money issuer the requisite level of confidence that the customer is the rightful holder of the card.
- Evidence of legitimate use. Seeking evidence of legitimate use is an alternative to establishing formal control over an account. An account that is used to fund an electronic money purse over a significant period of time is more likely to be used legitimately, as the passage of time gives the rightful owner the opportunity to discover fraudulent use of the product and to block its use, which would in turn become evident to the issuer. Thus, for some products, this may provide a means of establishing legitimate use of a funding instrument. However:
  - Such an approach is sensitive to the issuer's ability to monitor, track and record use of a funding instrument associated with an account, and issuers wishing to adopt this approach must therefore have systems that are appropriate for this purpose.
  - A minimum period of four months must elapse, together with significant usage in terms of number and value of transactions over this time, to satisfy the issuer that the instrument is being legitimately used.[5]

3.41. Electronic money issuers must have processes in place to ensure that additional due diligence measures are applied if the money laundering and terrorist financing risk posed by the product or customer increases.

[5] The four-month period should be completed before any limits associated with simplified due diligence are exceeded.

3.42. Information on the payer that is received as part of the obligations under the WTR may contribute to verifying a customer's identity.

Basic requirements under this guidance in relation to products benefiting from the e-money-specific exemption and those applying simplified due diligence

~~3.38.~~3.43. This guidance provides for additional measures in relation to the application of simplified due diligence. Issuers should adopt the following measures that relate to verification of identity and monitoring:

Verification of identity

~~3.39.~~3.44. Either the electronic money system is a 3-party scheme; or

It is a 4-party scheme, in which case all other participating issuers should under this guidance meet the following requirements:

a) In all cases merchants must be subject to due diligence measures in accordance with Part I, Chapter 5 (but see para~~graph~~. 3.~~61~~60 below for a limited exemption) or as required by an equivalent jurisdiction.

b) Where electronic money is accepted by merchants or other recipients belonging to a wider payment scheme (for example Visa or MasterCard), issuers must satisfy themselves that the verification of identity and other due diligence measures carried out by that scheme in relation to merchants are, in the UK, equivalent to those of this sectoral guidance; or for other jurisdictions, are subject to equivalent requirements.

c) Where redemption of electronic money is permitted by way of cash access, for example through withdrawal at ATMs or through a cash-back facility at retailers, and where controls cannot be implemented to prevent this ~~reaching/~~exceeding the ~~annual~~cash redemption limit ~~of €1,000 [£800]~~under the e-money-specific exemption or ~~single transaction~~any other cash redemption limit ~~of €1,000 [£800]~~associated with simplified due diligence, customer due diligence must be carried out at the point of issuance of the electronic money~~.~~ or before such functionality is enabled. Furthermore, issuers must, wherever possible, require all refunds made by merchants in the event of return of goods or services to be made back onto the electronic money purse from which payment was first made.

Monitoring

~~3.40.~~3.45. Issuers must establish and maintain appropriate and risk-sensitive policies and procedures to monitor business relationships and transactions on an ongoing basis. Part I Chapter 5 (see in particular section 5.7) sets out how this can be done.

~~3.41.~~3.46. If issuers wish to benefit from the e-money-specific exemption or the simplified due diligence provisions under this guidance, they must, in addition to the processes set out in part I Chapter 5, deploy specific minimum transaction monitoring and/or on-chip purse controls that enable control of the systems and recognition of suspicious activity. Such controls may include:

- Transaction monitoring systems that detect anomalies or patterns of behaviour, or the unexpected use of the product, for example frequent cross-border transactions or withdrawals in products that were not designed for that purpose;
- Systems that identify discrepancies between submitted and detected information – for example, between submitted country of origin information and the electronically-detected IP address;

- Systems that cross-reference submitted data against existing data for other accounts, such as the use of the same credit card or device by several customers;
- Systems that interface with third party data sources to import information that may assist in detecting incidence of fraud or money laundering across a number of payment service providers;
- On-chip controls that impose purse rules, such as those specifying the POS terminals or other cards with which the purse may transact;
- On-chip controls that impose purse limits such as transaction or turnover limits;
- On-chip controls that disable the card when a given pattern of activity is detected, requiring interaction with the issuer before it can be re-enabled;
- Controls that are designed to detect and forestall the use of the electronic money product for money laundering or terrorist financing in accordance with the typologies identified for such a product.

~~3.42.~~3.47. Information obtained through monitoring must be reviewed as part of the ongoing risk assessment; issuers must apply customer due diligence measures and monitoring appropriate to the risks.

~~3.43.~~ Issuers are reminded that in the event that potentially suspicious activity is detected by internal systems or procedures, they must must comply with their obligations under POCA and the Terrorism Act 2000~~, as amended by the Anti-terrorism, Crime and Security Act 2001~~ (see Part I, Chapter 6) to report possible money laundering or terrorist financing.

~~*Basic means of verification of identity (above SDD thresholds)*~~

~~3.44. As stated in paragraph 3.23 above, the Money Laundering Regulations 2007 require that customer due diligence measures are carried out on a risk-based approach, as set out in Part I, Chapter 5. Electronic money is issued in a range of products, for a range of purposes covering a spectrum of risk – from the purchase of goods and services, to person-to-person payments. An issuer's risk-based approach to customer due diligence measures will, as required by the Money Laundering Regulations 2007, be informed by a number of factors, including the type of product or transaction involved.~~

~~*Reliance on the funding instrument*~~

~~3.45. As part of a risk-based approach to verification of identity, the Money Laundering Regulations 2007 require that verification is carried out on the basis of 'documents, data or information obtained from a reliable and independent source'. In some cases, where the risk associated with the business relationship is low, a customer's funding instrument (such as a credit card or bank account) can constitute such data or information, subject to the following additional requirements:~~

~~a) The issuer remains ultimately responsible for meeting its customer due diligence obligations;~~

~~b) The issuer has in place systems and processes for identifying incidents of fraudulent use of credit/debit cards and bank accounts;~~

~~c) The issuer has in place systems and processes that enable monitoring to identify increased risk for such products, even within the permitted turnover limits. If the risk profile can then no longer be regarded as low risk, additional verification steps must be undertaken;~~

~~d) The issuer records and keeps records of relevant information, for example IP addresses, which assist in determining the electronic footprint of the customer, or where a POS~~

terminal is used in a face-to-face environment, records the correct use of a PIN or other data;

e) The funds to purchase electronic money are drawn from an account or credit card with, or issued by, a credit or financial institution[6] in the UK, the EU or an equivalent jurisdiction, which is supervised for its AML controls;

f) The issuer implements systems and controls to mitigate the risk of the funding card or account being itself subject to SDD;

g) The issuer has reasonable evidence to conclude that the customer is the rightful holder of the account on which the funds are drawn (which may be achieved using the processes described in paragraph 3.48 below);

h) The overall amount transacted by one customer does not exceed a maximum turnover limit of €15,000 [£12,500] from the commencement of the business relationship.

3.46. Where the above are not satisfied, further customer due diligence measures have to be applied.

3.47. A funding instrument on its own, however, is a weak form of verification of identity. The credit or financial institution whose evidence is being used may not have verified the customer to current standards, and there is a risk that the person using the account is not its rightful holder. This risk is even higher where an electronic money issuer has no evidence that the account is held in the same name as the customer, as is the case, for example, in relation to direct debits.

Establishing control over the funding instrument

3.48. Where payment is made electronically, it is usually not possible to verify the name of the account holder for the funding account. In this case, steps must be taken to establish that the customer is the rightful holder of the account from which the funds are drawn. These steps may include the following:

- Micro-deposit. Some issuers have developed a means of establishing control over a funding account using a process that is convenient and effective. A small random amount of money is credited to a customer's funding account and the customer is then required to discover the amount and to enter it on the issuer's website. By entering the correct value, the customer demonstrates access to the bank/card statement or accounting system of their bank or financial institution. This method, and its close variants (such as the use of unique reference numbers), provides an acceptable means of confirming that the customer has access to the account, and therefore has control over it. It also provides a means of guarding against identity theft, contributing therefore to the verification of identity process. If such an approach is not used, some other means of establishing control of the account is needed.

- Additional fraud checks. Issuers may also use additional fraud checks undertaken at the time of the transaction which seek to cross reference customer-submitted data against data held by the electronic money or card issuer or similar independent third party, and which gives the electronic money issuer the requisite level of confidence that the customer is the rightful holder of the card.

- Evidence of legitimate use. Seeking evidence of legitimate use is an alternative to establishing formal control over an account. An account that is used to fund an electronic money purse over a significant period of time is more likely to be used legitimately, as the passage of time gives the rightful owner the opportunity to discover fraudulent use of

[6] Other than a money service business, or a payment or electronic money institution providing mainly money remittance services.

~~the product and to block its use, which would in turn become evident to the issuer. Thus, for some products, this may provide a means of establishing legitimate use of a funding instrument. However:~~

- ~~Such an approach is sensitive to the issuer's ability to monitor, track and record use of a funding instrument associated with an account, and issuers wishing to adopt this approach must therefore have systems that are appropriate for this purpose.~~
- ~~A minimum period of four months must elapse, together with significant usage in terms of number and value of transactions over this time, to satisfy the issuer that the instrument is being legitimately used.~~[7]

~~3.49. Electronic money issuers must have processes in place to ensure that additional due diligence measures are applied if the money laundering and terrorist financing risk posed by the product or customer increases.~~

~~3.50.~~3.48. ~~Complete Information on the Payer (CIP), received as part of the obligations under the Wire Transfer Regulation, may contribute to verifying a customer's identity.~~

Enhanced due diligence

~~3.51.~~3.49. The Money Laundering Regulations ~~2007~~2017 require enhanced due diligence to be undertaken in all situations where the risk of money laundering is perceived to be high. These include instances where the customer is not physically present for identification purposes,[8] as well as in respect of business relationships or occasional transactions with politically exposed persons (PEPs).

~~3.52.~~3.50. Where electronic money purses are purchased or accounts opened in a non-face-to-face environment, issuers must take specific and adequate measures to address the greater risk of money laundering or terrorist financing that is posed (see Part I, ~~paragraphs~~paras. 5.~~5.10~~3.85 to 5.~~5.17 provide guidance~~3. 91 on ~~enhanced due diligence for~~the mitigation of impersonation risk arising from non-face-to-face transactions). Issuers may adopt means of verification other than those outlined in Part I, provided that these are commensurate to the risk associated with the business relationship.

~~3.53.~~3.51. The requirement for issuers to have systems and processes to detect PEPs will be proportionate to the risk posed by the business relationship, as will the degree of enhanced due diligence required for PEPs. Issuers should focus their resources in a risk sensitive manner on products and transactions where the risk of money laundering is high. Further guidance on the application of the risk-based approach to PEPs is provided in Part I, ~~paragraphs~~paras. 5.5.~~26~~24 to 5.5.~~30~~28.

~~3.54.~~3.52. In all other high risk scenarios, issuers should have regard to the guidance in Part I Chapter 5.

Multiple-card products

~~3.55.~~3.53. Issuers whose products enable two or more cards to be linked to a single account must establish whether they have entered into one or more business relationships, and must verify the identity of all customers with whom they have a business relationship.

~~7 The four-month period should be completed before the limits associated with simplified due diligence (see paragraph 3.29) are exceeded.~~

8 But note that if an electronic money purse meets the conditions for ~~simplified due diligence~~the e-money-specific exemption, no identification of the customer is required, even though the customer may not have been physically present. Outside the conditions for the e-money-specific exemption, this risk factor is merely one of many and may be mitigated against, see para. 3.16 above.

~~3.56.~~3.54. Issuers should also consider wether the functionality of the second card may give rise to benenficial ownership.

~~3.57.~~3.55. Where additional card holders remain non-verified, issuers must implement controls effectively to mitigate the greater risk of money laundering and terrorist financing to which these products are exposed.

Verification of identity – merchants

~~3.58.~~3.56. The FCA expects electronic money issuers to understand who their merchants are in order to guard against the risk that their electronic money products might be used for money-laundering or terrorist financing.

~~3.59.~~3.57. Issuers must therefore apply ongoing due diligence to merchants on a risk-sensitive basis in accordance with Part I, Chapter 5. This includes the requirement to undertake adequate due digligence on the nature of the merchant's business and to monitor the relationship.

~~3.60.~~3.58. In person-to-person systems, the boundary between consumers and merchants may be blurred; consumers may not register as merchants, but may nevertheless carry on quasi-merchant activity. In this case issuers:

- Should have systems in place that provide a means of detecting such activity.
- When such activity has been detected, apply due diligence measures appropriate to merchants.

~~3.61.~~3.59. Issuers may allow merchants to benefit from the €2~~,500 [£2,200]~~50 monthly turnover and €1~~,000 [£800]~~00 redemption allowance in order to enable the online recruitment of small merchants. This does not, however, alter the requirement to undertake adequate due diligence on the nature of the merchant's business.

Wire Transfer Regulation

~~3.62.~~3.60. ~~General provisions for compliance with~~ Guidance on the ~~Wire Transfer Regulation (Regulation (EC) 1781/2006 on information on~~ requirements of the ~~payer accompanying transfers of funds) are~~WTR is provided in Part I, ~~paragraphs~~paras. 5.2.~~10ff *Electronic Transfer of funds*,~~10 to 5.2.13 and in Part III, Specialist ~~guidance~~Guidance 1: ~~*Transparency in electronic payments (*~~*Wire transfers*~~).~~.

Scope

~~3.63.~~3.61. Issuers ~~are~~ may be subject to the ~~obligations~~requirements of the ~~Wire Transfer Regulation~~WTR in their role as PSP of the payer, PSP of the payee ~~and~~ or intermediary PSP. ~~An overview of these requirements is provided schematically at Appendix I to this guidance.~~

3.62. ~~Payments using~~Only those issuers that offer products that are used for person-to-person transfers or where the number of the e-money instrument does not accompany all transfers flowing from the transaction are subject to the requirements of the WTR.

~~3.64.~~ Where an electronic money ~~and~~ purse is funded through a card payment, this funding ~~of purses:~~

~~(i) Transactions up to €1,000 [£800] in value do not require the collection or sending of Complete Information on the Payer (CIP), as these transactions are subject to the exemption provided by Article 3(3)~~ transaction is a payment for goods and services and is therefore out of ~~the Wire Transfer Regulation.~~

3.63. ~~(ii) Transactions exceeding €1,000 [£800] in value require the collection, verification and sending of CIP on a risk-weighted basis[9] as set out elsewhere in this guidance or as set out at A1.9~~scope according to ~~A1.19~~Article 2(3) of the WTR (also see Part III, ~~Specialist guidance~~para. 1~~: *Transparency in electronic payments (Wire transfers)*.~~.17).

~~(iii) Where an electronic money purse is funded through a card payment exceeding €1,000 [£800], it has been agreed that for practical purposes such a transaction consitutes payment for goods and services under Article 3(2) of the Regulation, and consequently the sending of the card PAN number satisfies the requirement for a unique identifier to accompany the transfer of funds. See Part III, Specialist guidance 1: *Transparency in electronic payments (Wire transfers)*, paragraph 1.17. However, subsequent payments from the electronic money purse must be in accordance with (i) and (ii) above.~~

~~(iv) When funding transactions exceeding €1,000 [£800] are made from a bank account or other financial institution account in the EU, CIP can be substituted with an account number or a unique identifier enabling the transaction to be traced back to the payer (see Article 6 of the Wire Transfer Regulation).~~

Verification requirements under the WTR

3.64. Verification of information under the WTR should be undertaken using a risk-based approach as provided for elsewhere in this guidance or as set out in Part III.

3.65. Transactions up to €1,000 in value (single or linked) do not require the verification of the information on the payer by the PSP of the payer unless the funds are received in cash or anonymous e-money or there is a suspicion of money laundering or terrorist financing.

3.66. Transactions up to €1,000 in value (single or linked) do not require the verification of the information on the payee by the PSP of the payee unless the funds are paid out in cash or anonymous e-money or there is a suspicion of money laundering or terrorist financing.

~~3.65.~~ *Redemption of electronic money~~:~~*

3.67. ~~(i)~~ Payments made to customers in redemption of electronic money are usually made by bank transfer. Redemption comprises a payment by the issuer as principal (payer) to the electronic money account holder~~.~~ (payee). Issuers may, however, attach customer (in addition to their own) ~~CIP~~information as information on the payer to the redemption transaction in the usual way – benefitting from the provisions for inter EU payments where applicable, and ensuring additional information is available to the payee PSP.

~~(ii)~~ Where redemption is made in cash, this benefits from the exemption from the ~~Wire Transfer Regulation~~WTR for cash withdrawals from a customer's own account ~~provided by~~Article 3(7)(a).

~~3.66.~~3.68. ~~Verification of identity for CIP information should be undertaken on a risk-weighted basis as provided for elsewhere in this guidance or as set out in paragraphs A1.9 to A1.19 of Part III, Specialist guidance 1: *Transparency in electronic payments (Wire transfers*~~under Article 2(4)(a).

Use of agents and distributors

~~3.67.~~3.69. Issuers may distribute or redeem electronic money through an electronic money distributor or payment services agent. Payment services agents must be registered with the

~~[9] See recital 11 and Art. 5 of Regulation (EC) No 1781/2006.~~

FCA. Issuers are ultimately responsible for compliance with AML-related obligations where these are outsourced to their distributors and payment services agents. Issuers must be aware of the risk of non-compliance by their outsourced service providers and must take measures to manage this risk effectively.

~~3.68.~~3.70. Issuers should apply the same customer due diligence measures to distributors as they do to merchants.

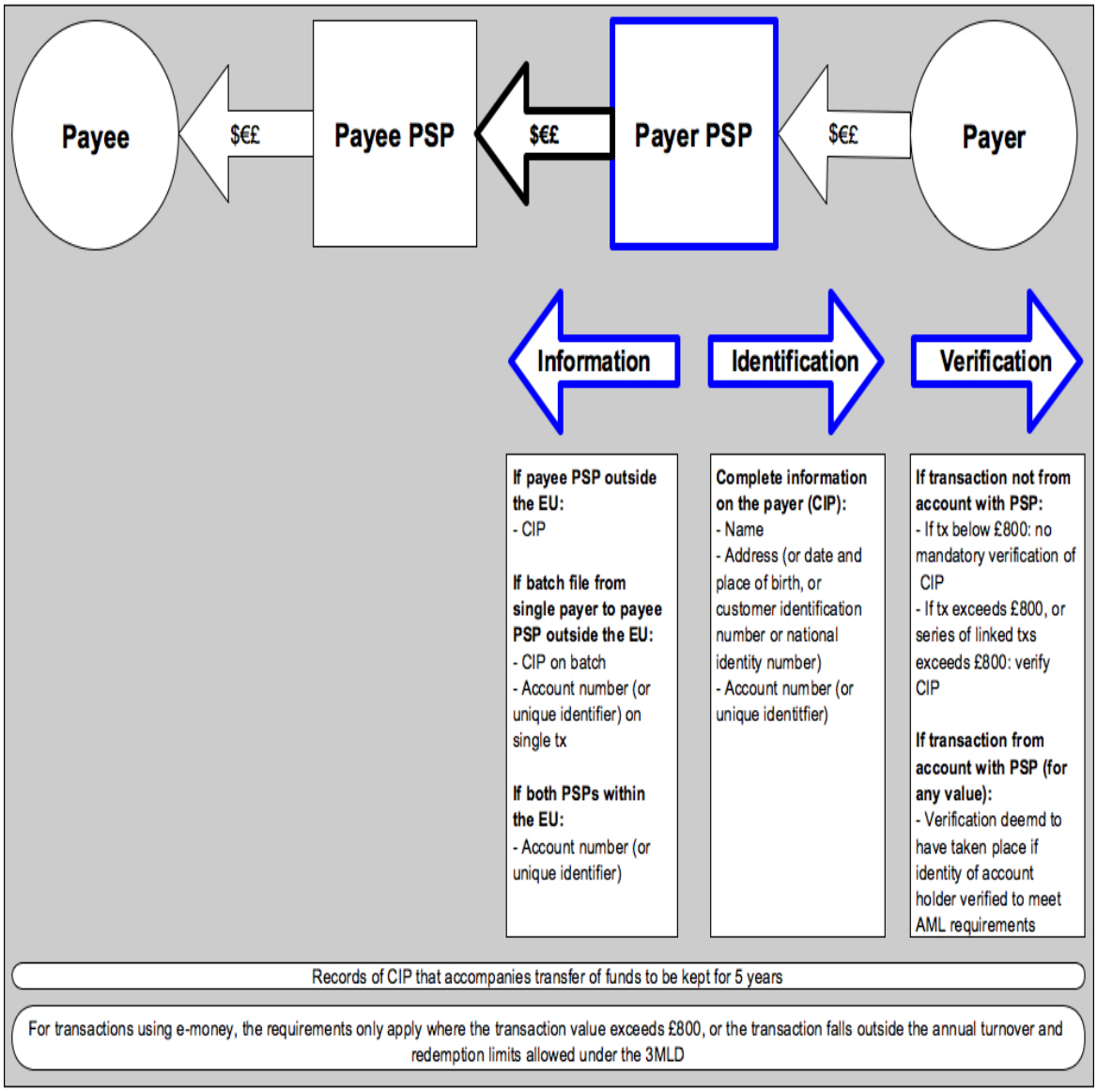
~~3.69.~~3.71. The FCA expects issuers to carry out fitness and propriety checks on payment services agents of electronic money issuers. These checks should include, among others, the assessment of the agents' honesty, integrity and reputation in line with Chapter 3 of the FCA's electronic money approach document.

~~3.70.~~3.72. Issuers are required to supply the FCA with a description of the internal control mechanisms their payment services agents have in place to comply with the Money Laundring Regulations ~~2007~~2017 and the Proceeds of Crime Act 2002. Where the payment services agent is established in another EEA jurisdiction, the issuer must ensure their AML systems and controls comply with local legislation and regulation that implements the ~~3~~4th Money Laundering Directive. Issuers must also take reasonable measures to satisfy themselves that their payment services agents' AML/CTF controls remain appropriate throughout the agency relationship.

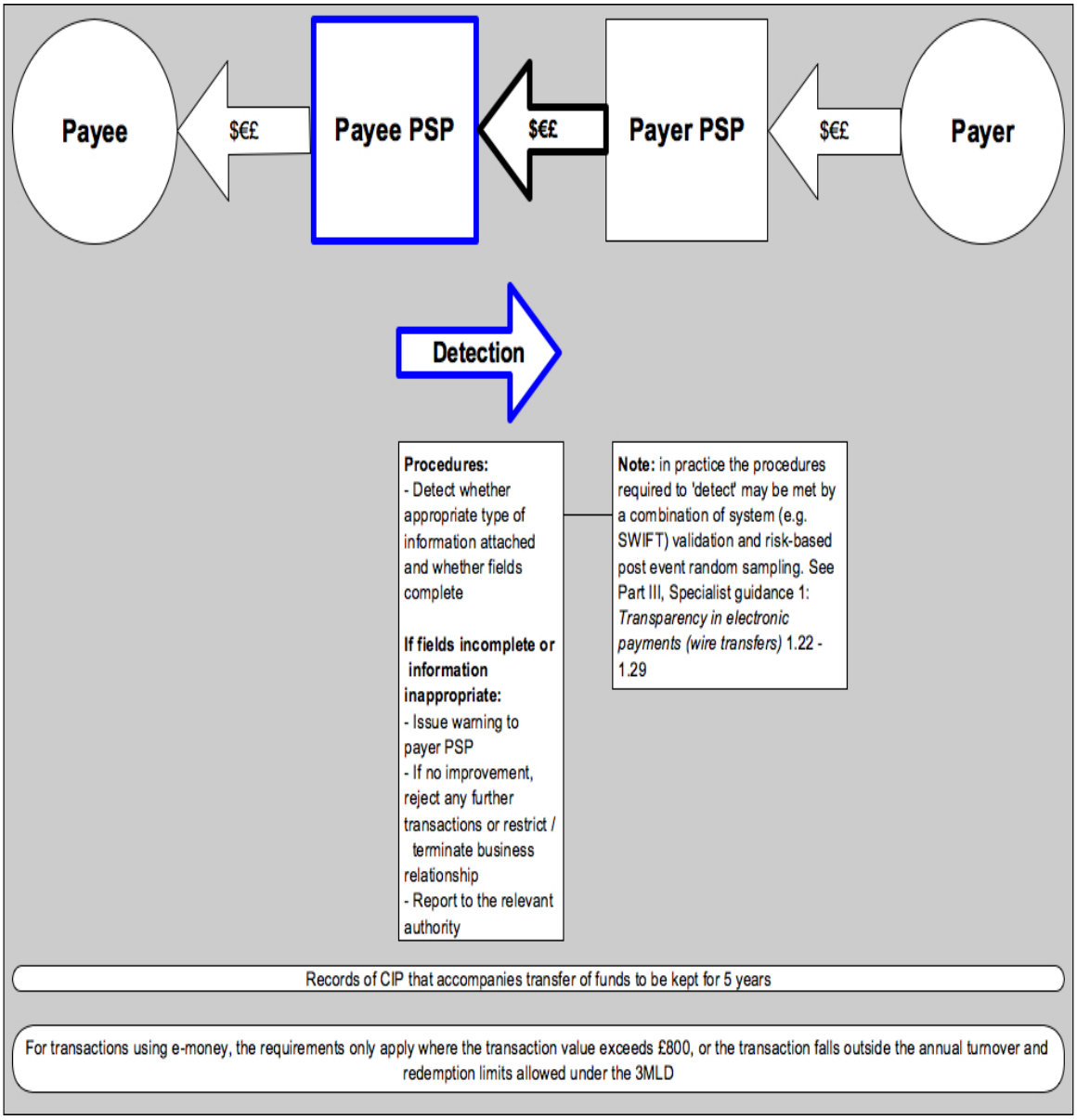
Central contact points

~~*Appendix I*~~

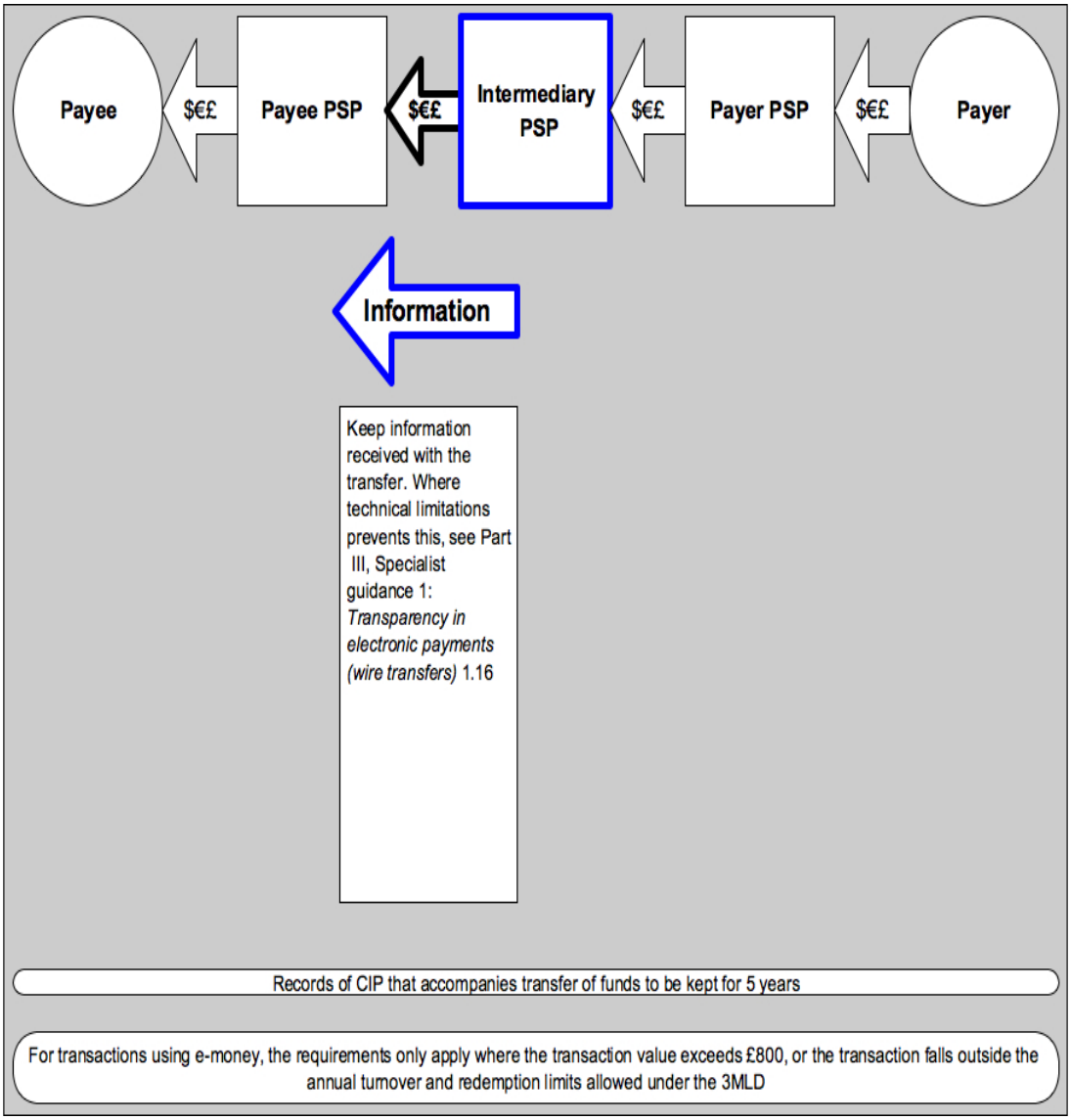
~~Scenario 1: Transfer of funds – Obligations on Payer PSP~~



~~Scenario 2: Transfer of funds – Obligations on Payee PSP~~



~~Scenario 3: Transfer of funds – Obligations on Intermediary PSP~~



3.73. Depending on their activities, when distributors or payment services agents are used to passport services to another EEA jurisdiction, these may be regarded as establishments in a form other than a branch and some member states may require issuers to establish a central contact point on their territory. The Joint Committee of the European Supervisory Authorities is developing regulatory technical standards for central contact points and these should be referred to when establishing and overseeing contact points.

3.74. What amounts to an establishment is defined in the Treaty, and guidance on the meaning of establishment has been issued by the European Commission in 1997.[10]

[10] Commission Interpretative Communication on Freedom to Provide Services and the Interest of the General Good in the Second Banking Directive (EC(97) 1193 final).