Electronic Money Association
Crescent House
5 The Crescent
Surbiton
Surrey
KT6 4BN
United Kingdom
Telephone: +44 (0) 20 8399 2066
Facsimile: +44 (0) 870 762 5063
www.e-ma.org

Ms Marianne Carrubba
Directorate-General for Justice and Consumers
European Commission
1049 Bruxelles
Belgium

17 March 2017

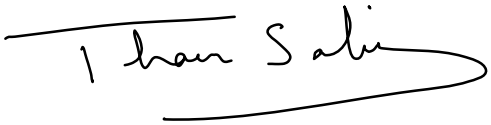
Dear Marianne

Re: Supranational risk assessment ("SNRA") of money laundering and terrorist financing risks affecting the EU

The EMA is the EU trade body representing electronic money issuers and alternative payment service providers. Our members include leading payments and e-commerce businesses in Europe that provide online payments, card-based products, electronic vouchers and mobile payment instruments. Most members operate across the EU, most frequently on a cross-border basis. A list of current EMA members is provided at the end of this document.

Please find below our comments on the draft SNRA of 9 March 2017, specifically in relation to the section dealing with electronic money. Please feel free to contact us should you have any question or require further information.

Yours faithfully



Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

Supranational risk assessment of money laundering and terrorist financing risks affecting the EU

General comments

We appreciate the opportunity to respond to the draft SNRA, and have set out our comments to specific sections below.

Overall, we have found the assessment to be focused on prepaid cards, and specifically on those benefiting from the exemption from identification and verification. These continue to be a significant but small part of the business of e-money issuers overall.

Furthermore, there appears to be a perception that the industry is ill prepared for the risks that it faces and perhaps underfunded to deal with the challenges. This is not our experience; most businesses would fail very quickly if they did not devote sufficient resources to meet the challenges of financial crime including ML and TF.

Our association was established in 2001, and has met monthly since then to discuss regulatory and operational issues. We regularly hold AML sub-committee and Fraud sub-committee meetings. These have developed typologies, and have issued guidelines that are published as part of the UK Joint Money Laundering Steering Group guidance. These are drafted by industry but approved by UK Treasury Ministers and negotiated with law enforcement, FIU and competent authorities. These guidelines require the implementation of a range of controls by issuers as a condition of benefiting from SDD. These are in addition to the turnover limits set out in legislation.

There are also statements made a number of times that issuers of SDD prepaid cards are preoccupied with financial inclusion so as to compromise their risk awareness and lead to an assessment of ML risk as being marginal. We again do not recognize this statement, and do not see any variation in the approach to risk assessment and mitigation for any e-money product. Issuers adopt a multi-level approach to risk assessment and mitigation as follows:

(i) At product design, the functionality is restricted to that absolutely necessary for the business proposition; removing ATM functionality if not needed, pacing a storage and transaction limit as needed by the product proposition, and placing restrictions of geographic or merchant usage as necessary.

(ii) Once in use, monitoring at consumer level for departures from the intended purpose, whether by value, frequency, location or funding and redemption. Similarly for merchants and for distributors, the values and frequency of transactions are monitored against baseline expectations and comparator outlets.

(iii) At a system level, patterns of behavior are monitored, seeking to identify typologies of ML or TF (where available); such as frequent low value transactions below a given threshold, pooling of funds, unusual withdrawals, changes to personal data etc. Also, systems seek to identify user credentials that are used multiple times, such as common passwords or user names, credit card numbers, addresses, IP addresses etc.

Section: Description of the sector

A significant part of the EU e-money industry is based in the UK, and UK data does not appear to feature in the ECB data used to describe the sector. This means that data is skewed towards online e-money account providers based in Luxembourg and prepaid card issuers based in Italy.

Furthermore, and in relation to SARs made by the sector, many FIUs including that based in the UK do not distinguish SARs made by e-money issuers from those made by other payment or banking service providers. This means that the significant number of SARs made by the industry have not been accounted for.

This is in contrast to the conclusions drawn at the end of the section stating:

"While the level of awareness of the sector to ML risks seems higher than for TF, the structure of the sector and its capability to provide for dedicated resources and training is quite low. Level of STRs confirmed this point."

The number of dedicated compliance staff at most issuers is significant, and is proportionate to the size of each business.

Section: Description of risk scenario

(i) This section is entirely focused on risks arising specifically from the limited opportunity for simplified due diligence, and adds risks associated with identity fraud – which is common to all financial services sectors.

(ii) The risk assessments and typologies developed by industry are more extensive. We have set out an extract from the set of typologies as a high level diagram at Annex 1 of this document. Each limb of the mind map represents a range of typologies that have been identified, and one or two examples have been provided for each.

(iii) This section also states that perpetrators can load multiple cards with substantial values which can then be transported abroad with limited traceability. This is not the case for the following reasons:

a. All cards have specific consumer propositions, and if used outside this scenario, will show up as unusual and be reported as suspicious. Transactions and accounts may also be frozen as a precaution.

b. Cards that are intended for cross border use and which can utilise ATMs such as travel money products are subject to full CDD at the outset. This was confirmed with issuers.

c. Electronic payments are traceable, and e-money products that require loading and are visible at the point of transaction are also traceable. Even if a user has not been identified, other information is available to trace transactions to an individual.

Section: Threat of TF

(i) This entire section is focused on prepaid cards that are fall within the limited scope of exemption for identification and verification. The conclusion however encompasses all e-money products. It states:

"e-money is attractive for terrorist groups as it allows financing terrorist activities easily and with a low level of planning/expertise."

(ii) There is limited evidence that prepaid cards were used by terrorists in paying for hotels or car rental – where they would also have had to offer separate evidence of ID. Furthermore, we understand that the cards were subject to identification and verification. Terrorists also use bank accounts and credit cards, as was evident in the London bombings, but this does not characterise such products as being 'attractive' for such groups.

(iii) Most significantly, other e-money products such as e-money wallets, mobile payment products and cards subject to CDD from the outset are all types of e-money that do not offer the characteristics described in this section. The conclusion is therefore not representative of the industry and of e-money products.

We would also draw the attention of the Commission to the impact of substituting prepaid cards benefiting from SDD for cash. The loss of opportunity for LE to make use of the transparency of electronic payment instruments, including those benefiting from SDD could be significant.

Section: Threat of ML

The emphasis is again on prepaid cards and on those benefiting from SDD. This has led to specific typologies being suggested, which can in fact be detected and mitigated against relatively easily.

The section states that the number of transactions is high and that this in itself represents an attractive MO for criminal organisations. There is no indication of what counts as 'high'. E-money transaction volumes are far lower than those undertaken using bank accounts or other payment instruments. The type of transactions is also relevant: how would a criminal organisation benefit from high levels of transactions that relate to low-risk purchases of goods and services?

As described in our typology extract, the risks of ML are in fact far more diverse, and have been tracked and mitigated by industry over a period of some 15 years.

There is reference to amounts around EUR 600 as 'large amounts'. This is certainly at the higher end of what is purchased by users, but is relatively low in objective terms when compared to other financial products and when considering the risk of ML.

We would be grateful for information on the laundering of the proceeds of drugs using e-money or the conversion of gold into e-money value. Such activity would show up on issuers' monitoring systems, and e-money offers a very poor means of undertaking such ML. The values loaded would be unusual, the pattern of loading, spending and redemption would be unusual, and the geographic locations would not fit the usual usage patterns.

We therefore challenge the conclusion that that e-money is attractive for criminals.

Section: Vulnerability TF

a) Risk exposure: reference is made to 'new technologies', 'widespread use', 'significant flows', 'speedy', 'anonymous' and 'sometimes cash-based', without providing any product examples that have all these characteristics. None to our knowledge exist. If they did, they would be vulnerable to fraud and would fail within a very short period of time for commercial reasons.

- In reality, cash-based products are restricted in value, allow for limited withdrawals without CDD and involve enhanced monitoring.

- Widespread use is made up of many specific product propositions that have well defined purposes, and each with its own control structure, and behaviour characteristics: travel cards are always subject to CDD, shopping mall cards are always used in a specific location, gift cards for a specific sector do allow for ATM usage and are used to purchase defined products; online wallets as a means to combine traditional payment products (bank account or card funding) with the convenience of prepopulated registered addresses.

- The scenarios contemplated by this section are not founded in real products, and could not be found in real products that are commercially viable.

The statement regarding the low values involved in TF does not assist in understanding vulnerability. The purchases referred to are almost always legitimate in appearance, and cannot indicate that TF activity is contemplated. This scenario is common to all payment products, and is not a vulnerability.

The ability of payment service providers to assist LE in detecting or monitoring TF subjects is dependent on additional intelligence being provided to the PSP, so accounts can be monitored, restricted or frozen. Alternatively, PSPs can offer help in identifying networks in the aftermath of an incident. This is again common to both e-money and other electronic payment products.

b) Risk awareness:

(i) The following statement is made at the outset:

"The promotion of e-money products in the field of financial inclusion or vulnerable people impacts the risk awareness of the sector which tends to consider ML abuses as marginal. Thus, the sector tends to advocate that due to the low level of ML risks, simplified CDD are adequate."

We would like to stress that products which are aimed at enhancing financial inclusion and targeted at vulnerable people may constitute a low risk of ML/TF, but that an overall risk assessment will always be undertaken.

As stated above, e-money products are associated with specific consumer propositions which feed into their risk assessment. Risks are mitigated through the application of relevant controls, and where residual risk is low, the application of SDD provisions is helpful in making e-money products accessible to the market.

(ii) CDD is described in brackets as "no identification, no verification", whereas 3MLD defines this more broadly and specifically requires ongoing monitoring of both the business relationship and scrutiny of transactions.

This is a key condition of the adoption of SDD, and serves to mitigate some of the risks. We have set out the role of monitoring elsewhere in this document for both verified and SDD products. The statement that in the absence of identification and verification, monitoring is not sufficient to identify suspicious transactions is not accurate. Monitoring is the basis for identifying unusual activities in the purchase, use or redemption of such products. Many SARs are made that relate to SDD products, or products for which SDD is part of their life cycle.

The conclusion to this section states: *"However, from a more general point of view, the sector is still not well organised and tends to have limited resources to provide guidance, training or dedicated staff."*

We do not recognise this statement, and would be interested in the data upon which it is based. As set out elsewhere, financial regulatory compliance including financial crime compliance are a high priority for all regulated EMIs and credit institution issuers, and this is reflected in resource allocation and participation in EMA specialist sub committees.

c) Legal framework and controls

The assessment makes the following statement in relation to cross-border activity:

"However, many electronic money institutions operate cross-border in the EU. In that context, the supervision of the sector is not considered as robust enough to address the risks. New risks and opportunities may emerge with FinTech/RegTech."

It is not clear what risks are not addressed in the context of cross border offering of services. Issuers operate their risk systems centrally, and are able to monitor and deploy controls in this way. All transactions are visible to the issuer and can be included in the risk management framework. There are generic risks associated with non-face-to-face engagement with customers, and these are addressed as part of the overall risk framework.

Where issuers utilize distributors to act as sales intermediaries in other member states, the business activity undertaken by distributors is minimal, and compliance obligations are generally not outsourced to distributors. CDD, monitoring and oversight are better addressed by the issuer centrally, and only the issuer has sight of transactions that are undertaken with the products, of global purchase behavior (across multiple distributors), and of user data solicited or detected through systems, and they are consequently in an ideal position to exercise compliance related processes and controls.

In some instances, such as the distribution of travel prepaid cards, CDD is undertaken at the outset. In these situations, distribution is only undertaken through licensed entities or agents subject to AML obligations, and subject to requisite training to undertake CDD processes.

The conclusion of this section states:

"When used anonymously, e-money is inherently exposed to TF vulnerability. The level of awareness of the sector is increasing but not in a sufficient way to allow FIUs to get enough data coming from suspicions transactions."

We are not in agreement with inherent vulnerability, as transactions are visible and unusual behaviour can be investigated. We believe it is equally challenging for any other payment product to identify a hotel booking or car rental as being related to TF.

Again anonymous prepaid cards appear to be the focus of the analysis, to the exclusion of all other e-money products. We believe the analysis of prepaid cards does not adequately consider controls and mitigation strategies deployed. Views formed in relation to a narrow part of the sector should not be the basis of conclusions for the entire e-money industry, much of which is not card-based, nor employs SDD provisions.

Section: Vulnerability ML

(a) Risk exposure: please refer to our comments on the same section relating to TF; similar language is used here which does not relate to industry practice.

(b) Risk awareness: similar comments to those under TF, suggesting low risk awareness and a focus on financial inclusion as the basis for applying SDD when this is not justified by low risk.

The industry has been undertaking risk assessments on ML and TF since 2001, and has collated typologies and published guidance. The ML overview of typologies appears at Annex 1, and Annex 2 provides the e-money sector specific guidance on CDD, which is published as part of the UK Joint Money Laundering Steering Group and which is drafted and adopted by members of the EMA.

Please note that JMLSG Guidance is comprised of three parts, a general Part 1 which e-money issuers also refer to, and a Part 3 on TF which again issuers refer to.

Although the guidance is set out for UK authorised firms, it applies to all EMA member firms, irrespective of their jurisdiction of authorisation.

I would like to draw your attention to the sections on SDD in the JMLSG guidance at paragraphs 3.30 to 3.43, which set out in some detail the conditions that EMA member issuers must fulfil in order to benefit from SDD under the guidance; requirements that go beyond those in 3MLD.

(c) Legal framework and controls:
In our experience, most LEAs and CAs that regard the regime as inadequate adopt a different view once they have been informed of the product details, risk management framework, and controls deployed. The nature of the product and technology means that it is easy to see theoretical vulnerabilities, but these are invariably addressed during product design, implementation and operation.

We disagree that "e-money is inherently exposed to ML when used anonymously". WE reassert that the controls implemented deter and detect most incidents of abuse that do occur, as demonstrated by the typologies documented by industry and ongoing SAR and LE engagement.

Conclusions
We thank the Commission for the opportunity to respond to the draft SNRA, and have set out our views in this document.

We believe the assessment focuses on anonymous prepaid cards to the exclusion of the main part of the industry, resulting in a skewed overall assessment.

We believe the Commission has underestimated the knowledge, know how, skill and resourced deployed by industry since 2001 in understanding, developing guidance and sharing information on ML and TF risks, and also in making SARs/STRs.

We also believe the Commission has overestimated the risks associated with the use of SDD by some products either during part of their lifecycle or for the product as a whole, given the additional controls that are required to be deployed (see EMA JMLSG Guidance) and the ability to deter and detect abuse.

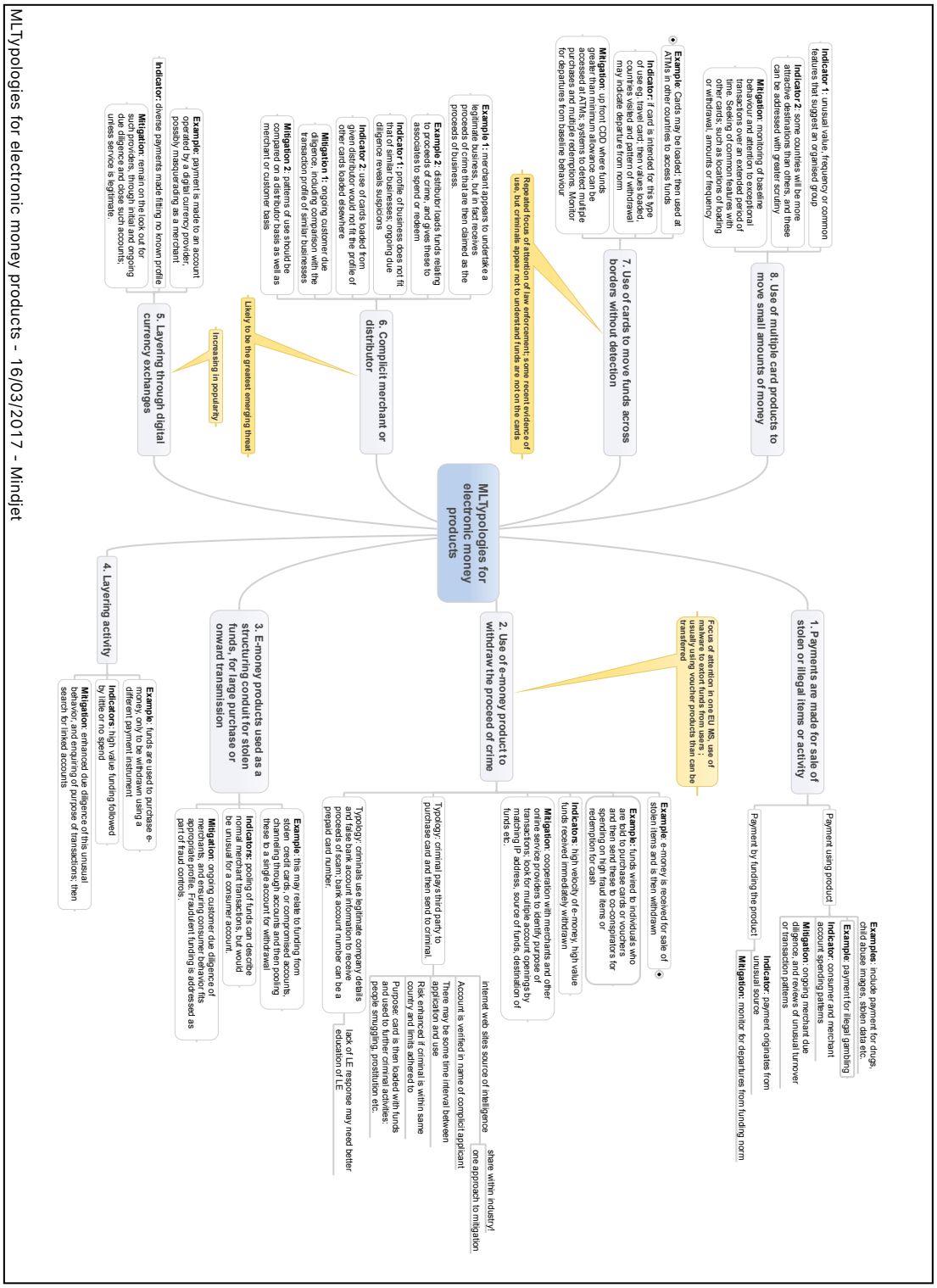
We would be grateful if our comments could be take into account when finalizing the SNRA with respect to e-money, and to take into account the know-how, guidelines and engagement that industry has devoted since 2001.

Mitigation: We believe that 4MLD and potentially 5MLD address many of the perceived risks set out in the document in relation to exemption from identification for prepaid cards; as the limits have been reduced.

We similarly believe that industry guidance, including the update that will take place over the next months in preparation for 4MLD will address any remaining concerns by setting out good practice in a similar manner to the current text.

Finally, industry information sharing, development of typologies, engagement with FIUs and other public bodies will assist in further addressing the risks of ML and TF that arise.

Annex I Overview and samples of ML Typologies



MLTypologies for electronic money products - 16/03/2017 - Mindjet

Annex II Electronic Money CDD Sector Guidance for ML and TF

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 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 card-based or an online account-based product.

3.4. The Electronic Money Regulations 2011 also provide for a number of exemptions (see paragraph 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 FSA, or it may be issued by specialist electronic money institutions, who obtain an authorisation from the FSA 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 FSA as small electronic money institutions.

3.6. All issuers of electronic money are subject to the Money Laundering Regulations 2007, section 21 A of the Terrorism Act, the EC 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 FSA's handbook.

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 of the Payment Services Directive (2007/64/EC) 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 trade body representing electronic money issuers and 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.

- **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 defined in Article 2(5) of the Wire Transfer Regulation as "a natural or legal person whose business includes the provision of 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 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 Regulation]:**

  Regulation (EC) 1781/2006 on information on the payer accompanying transfers of funds implements Special FATF Recommendation VII in EU 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, whether through the purchase of electronic money, 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. 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. 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. 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. 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. 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.

3.16. A non-exhaustive list of risk factors that may apply to electronic money products is given in paragraph 3.19 below; risk mitigating factors are listed in paragraph 3.21 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 Part I 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 transaction monitoring systems.

3.17. 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.

3.18. Issuers will need to evidence that they deploy an adequate range of controls to mitigate the ML/TF risks they encounter.

Risk factors

3.19. 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 paragraph 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 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[1];
- 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;
- 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. Absence of any of the above factors will decrease the risk.

Risk mitigating factors

3.21. 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. 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 document;
- Will detect anomalies to normal transaction patterns;

[1] 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).

- 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;
- 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. The Money Laundering Regulations 2007 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. 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. 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 5.3.98 to 5.3.114.

3.25. Issuers will also need to satisfy themselves that they comply with sanctions legislation. Guidance on this is provided in Part I, paragraphs 5.3.41 to 5.3.64, and Part III, 4.

Verification of identity – consumers

3.26. 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.

3.27. In addition to normal customer due diligence, the Money Laundering Regulations 2007 specify circumstances where simplified due diligence can be applied. Simplified due diligence is 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.

A purse must meet specific storage, turnover and redemption limits in order to qualify for simplified due diligence (see paragraphs 3.30 to 3.37 below), and issuers must have systems and controls in place to make sure these limits 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. Issuers should also comply with the requirements set out paragraphs 3.38 to 3.42 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.

3.29. 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 3.51 to 3.54 below).

Simplified due diligence

3.30. The Money Laundering Regulations 2007 (Reg. 13(7)(d)) distinguish between 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, the maximum amount stored in the device is no more than 250 euro or, in the case of electronic money used to carry out payment transactions within the United Kingdom, 500 euro; or*
>
> *(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).'*

Non-reloadable purses

3.31. Electronic money purses that cannot be recharged, and whose total purse limit does not exceed €250 [£200] or €500 [£400] for payment transactions within the United Kingdom, benefit from simplified due diligence.

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, 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].

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 the 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
- Where the issuer suspects money laundering or terrorist financing.

Basic requirements under this guidance in relation to simplified due diligence

3.38. 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. 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 paragraph 3.61 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 redemption limit of €1,000 [£800] or single transaction limit of €1,000 [£800], customer due diligence must be carried out at the point of issuance of the electronic money. 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. Issuers must establish and maintain appropriate and risk-sensitive policies and procedures to monitor business relationships on an ongoing basis. Part I Chapter 5 (see in particular section 5.7) sets out how this can be done.

3.41. If issuers wish to benefit from 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 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. 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[2] 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 against 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

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

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.[3]

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. 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.

1.1.1

1.1.2 Enhanced due diligence

3.51. The Money Laundering Regulations 2007 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,[4] as well as in respect of business relationships or occasional transactions with politically exposed persons (PEPs).

3.52. 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 (Part I, paragraphs 5.5.10 to 5.5.17 provide guidance on enhanced due diligence for 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. 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

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

[4] But note that if an electronic money purse meets the conditions for simplified due diligence, no identification of the customer is required, even though the customer may not have been physically present.

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 5.5.26 to 5.5.28.

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

Multiple-card products

3.55. 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.

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

3.57. 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. The FSA 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. 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. 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. Issuers may allow merchants to benefit from the €2,500 [£2,200] turnover and €1,000 [£800] 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.

1.1.3 Wire Transfer Regulation

3.62. General provisions for compliance with the Wire Transfer Regulation (Regulation (EC) 1781/2006 on information on the payer accompanying transfers of funds) are provided in Part I, paragraphs 5.2.10ff *Electronic Transfer of funds*, and Part III, Specialist guidance 1: *Transparency in electronic payments (Wire transfers)*.

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

3.64. Payments using electronic money and 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) of the Wire Transfer Regulation.

(ii) Transactions exceeding €1,000 [£800] in value require the collection, verification and sending of CIP on a risk-weighted basis[5] as set out elsewhere in this guidance or as set out at A1.9 to A1.19 of Part III, Specialist guidance 1: *Transparency in electronic payments (Wire transfers)*.

(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).

3.65. Redemption of electronic money:

(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. Issuers may, however, attach customer (in addition to their own) CIP 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 for cash withdrawals from a customer's own account provided byArticle 3(7)(a).

3.66. 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)*.

1.1.4 Use of agents and distributors

3.67. Issuers may distribute or redeem electronic money through an electronic money distributor or payment services agent. Payment services agents must be registered with the FSA. 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. Issuers should apply the same customer due diligence measures to distributors as they do to merchants.

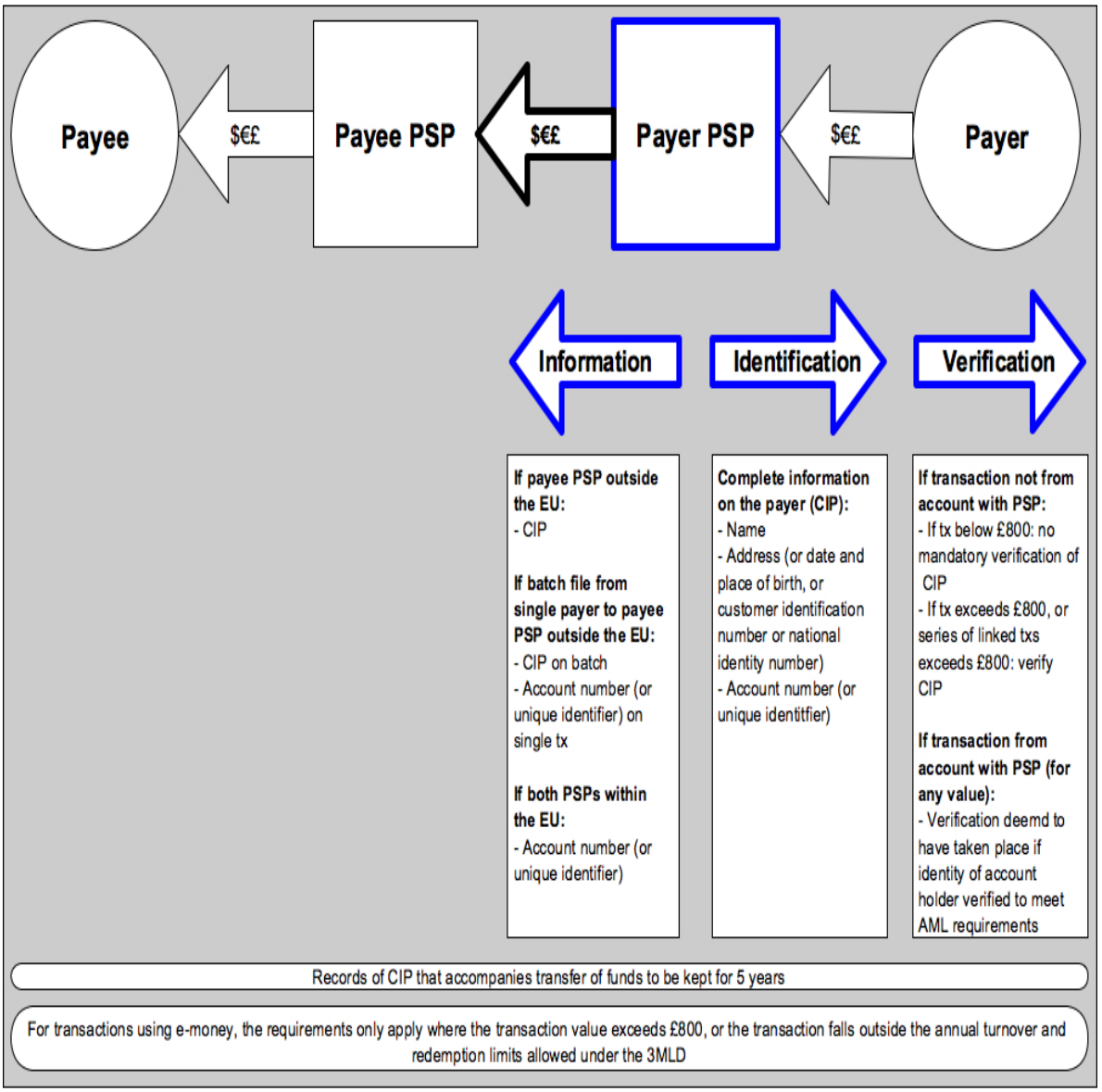
3.69. The FSA expects issuers to carry out fitness and propriety checks on payment services agents of electronic money issuers. These checks should include, among others, the assessment of the agents' honesty, integrity and reputation in line with Chapter 3 of the FSA's electronic money approach document.

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

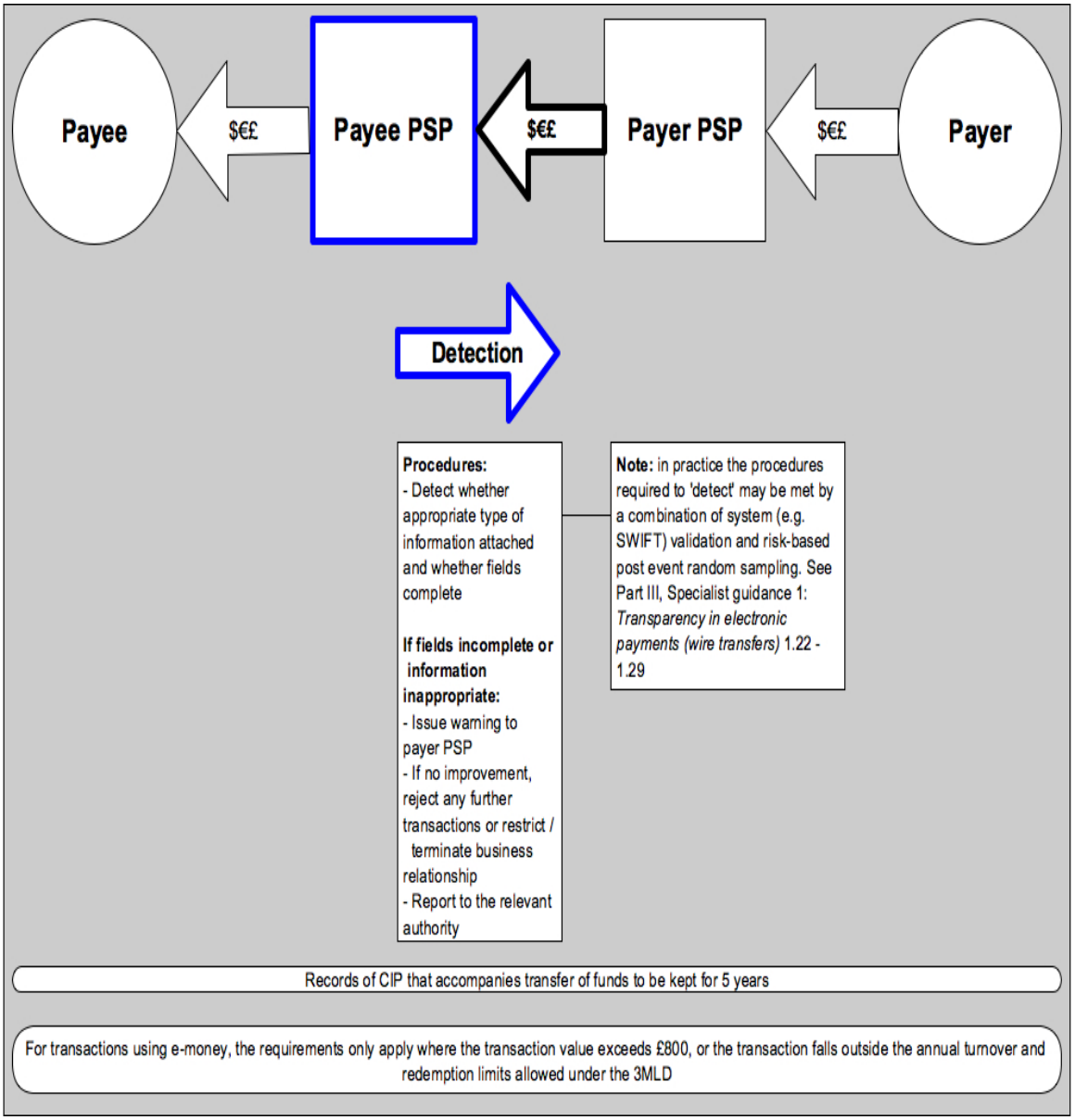
3.70. Issuers are required to supply the FSA with a description of the internal control mechanisms their payment services agents have in place to comply with the Money Laundring Regulations 2007 and the Proceeds of Crime Act 2002. Where the payment services agent is established in another EEA jurisdiction, the issuer must ensure their AML systems and controls comply with local legislation and regulation that implements the 3rd 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.

1.1.5 Appendix I

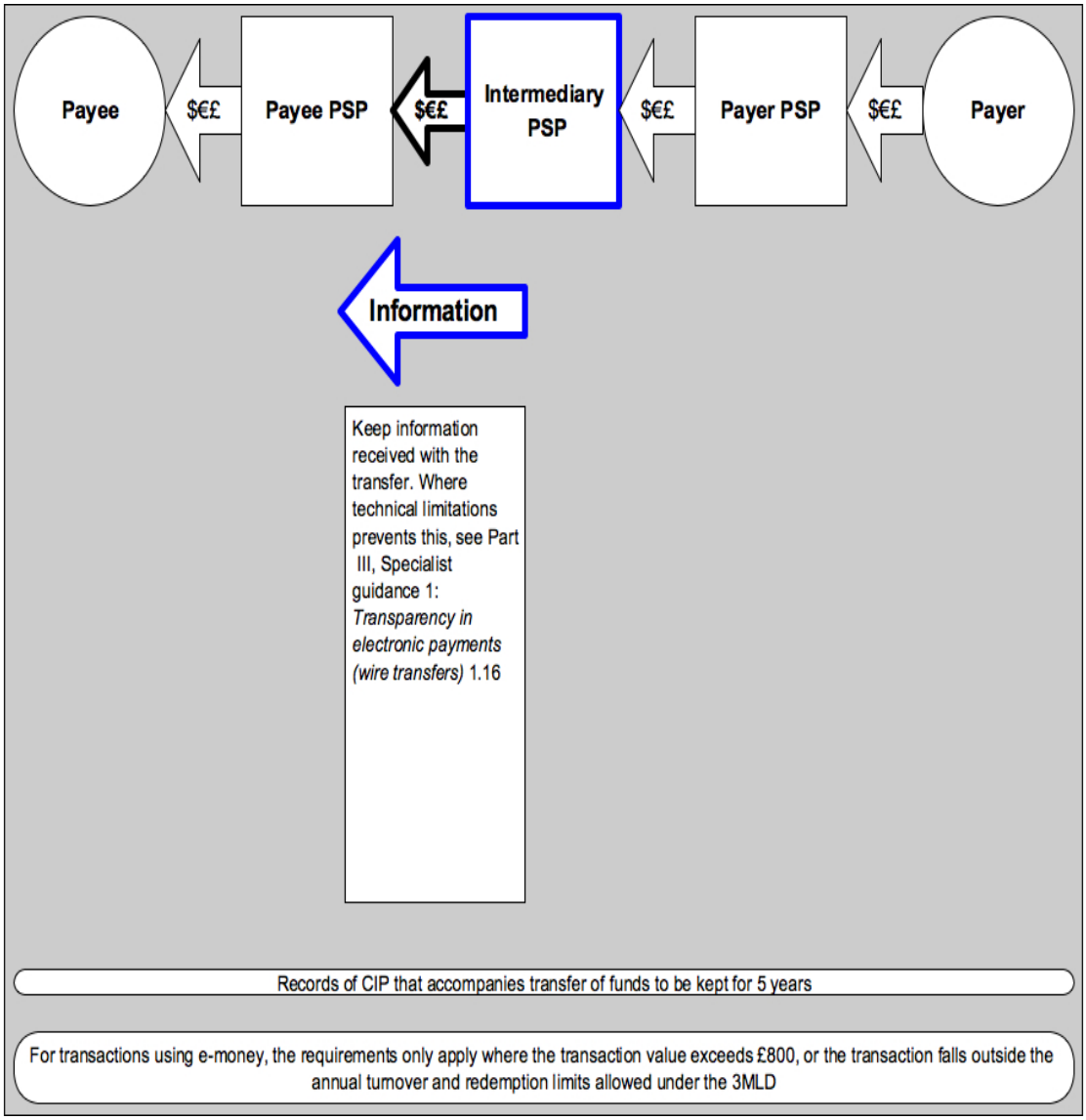
Scenario 1: Transfer of funds – Obligations on Payer PSP



Scenario 2: Transfer of funds – Obligations on Payee PSP



Scenario 3: Transfer of funds – Obligations on Intermediary PSP



List of EMA members as of March 2017:

24 Money
Advanced Payment Solutions Ltd
Airbnb Inc
Allegro Group
American Express
Azimo Limited
Bitstamp
Blackhawk Network Ltd
Boku Inc
Citadel Commerce UK Ltd
Clydesdale Bank
Coinbase
Corner Banca SA
eBay Europe Sarl
Euronet Worldwide Inc
Facebook Payments International Ltd
FaceKart
First Rate Exchange Services
Flex-e-card
Flywire
GoCardless Ltd
Google Payment Ltd
iCheque Network Limited
IDT Financial Services Limited
Imagor SA
Ixaris Systems Ltd
Kalixa Pay Ltd
MarqMillions
Merpay Ltd.
One Money Mail Ltd
Optal
Park Card Services Limited
Payfriendz Ltd
Payoneer
PayPal Europe Ltd
PayPoint Plc
Paysafe Group
PPRO Financial Ltd
PrePay Solutions
R. Raphael & Sons plc
Remitly
SafeCharge UK Limited
Securiclick Limited
SEQR
Skrill Limited
Stripe
Syspay Ltd
Transact Payments Limited
TransferWise Ltd
Valitor
Wave Crest Holdings Ltd
Wirecard AG
Worldpay UK Limited