Payment Services and Electronic Money – Our Approach

The FCA's role under the Payment Services Regulations 2017 and the Electronic Money Regulations 2011

DRAFT

April 2017

Preface

This document will help businesses navigate the Payment Services Regulations 2017 (PSRs 2017), the Electronic Money Regulations 2011 (EMRs) together with our relevant rules and guidance, and to understand our general approach in this area. It is aimed at businesses that are, or are seeking to become:

- authorised payment institutions or small payment institutions (collectively - PIs)
- authorised e-money institutions or small e-money institutions (collectively - EMIs)
- registered account information service providers (RAISPs)
- credit institutions, who must comply with parts of the PSRs 2017 and EMRs when carrying on payment services and e-money business

The first version of the Payment Services Approach Document was issued in April 2009 and since then we have kept the document under review and have updated it to clarify our interpretation of the Payment Services Regulations 2009 (PSRs 2009), and answer businesses' questions. When the second Electronic Money Directive (2EMD) was implemented in the UK on 30 April 2011 through the EMRs, we produced a separate approach document for the e-money regime.

This April 2017 Approach Document has been updated throughout to reflect the following:

- changes brought about by the introduction of the revised Payment Services Directive (PSD2)
- changes in the market that have an impact on the guidance we first published in 2009 and 2011 respectively
- the feedback received in the course of the Call for Input we published in February 2016

Our decision to merge our Approach Documents on the PSRs 2017 and the EMRs is an important outcome of the Call for Input.[1]

We consulted on these changes in April 2017. Our consultation papers and feedback statements can be accessed on our website.

[1] Previously, "The FCA's role under the Payment Services Regulations 2009" and "The FCA's role under the Electronic Money Regulations 2011" respectively

Contents

1. Introduction

1.1. This document describes our approach to implementing the PSRs 2017, the EMRs and the small number of payment services and e-money-related rules in our Handbook of Rules and Guidance (the Handbook). It gives readers a comprehensive picture of the payment services and e-money regulatory regime. It also provides guidance for a practical understanding of the requirements, our regulatory approach and how businesses will experience regulatory supervision.

1.2. We use a number of similar terms with distinct meanings in this document. The glossary of terms, abbreviations and acronyms at the end provides a full list.

1.3. PSD2requires the European Banking Authority to produce a number of technical standards and guidelines for the implementation of the directive. Where relevant, these standards and guidelines should be read alongside this document.

1.4. The Payment Systems Regulator has published a separate Approach Document on the aspects of the PSRs 2017 which it is solely responsible for, including access to payment systems, and information to be provided by independent ATM deployers.

The payment services and e-money regulatory regime

1.5. The regime implements PSD2 and 2EMD. As with the first Payment Services Directive, PSD2 and 2EMD (and their implementing regulations) are closely interlinked. Most e-money issuers will be carrying on payment services in addition to issuing e-money so will need to be familiar with both the PSRs 2017 and the EMRs, including the changes made as a result of the implementation of PSD2.

Payment Services

1.6. PSD2 was published in the European Union's Official Journal on 23 December 2015. It replaces an earlier payment services directive (PSD1) and updates the regulatory regime to reflect changes in the market and remove barriers to market entry. The main changes are summarised below. Its aims include:

- contributing to a more integrated and efficient European payments market
- levelling the playing field for payment service providers
- promoting the development and use of innovative online and mobile payments
- making payments safer and more secure
- protecting consumers
- encouraging lower prices for payments

1.7. PSD2 will continue to govern the authorisation and prudential requirements for PIs and set the conduct of business rules for providing payment services.

1.8. The PSRs 2017 [Draft PSRs 2017] and parts of the Handbook implement PSD2 in the UK. Most payment service providers are required to be either authorised or registered by us under the PSRs 2017 and to comply with certain rules about providing payment services, including specific requirements for payment transactions.

1.9. The PSRs 2017 replace the PSRs 2009 and make the following changes to the regulatory regime:

- Amend the authorisation and prudential regime for payment service providers and e-money issuers that are not banks or building societies (and so otherwise authorised by us). Such businesses are known as authorised payment institutions (authorised PIs) and authorised e-money institutions (authorised EMIs). Authorised PIs and authorised EMIs can passport their services to other EEA States – because of their UK authorisation, they have the right to establish or provide services across the EEA. The exercise of passporting rights is amended through the PSRs 2017 as well as EBA Regulatory Technical Standards on passporting under PSD2. Further information can be found in **Chapters 3 – Authorisation and registration, 6 – Passporting and 9 – Capital resources and requirements**.

- Continue to allow payment service providers operating beneath a certain average monthly turnover threshold to be registered instead of obtaining authorisation (regulation 14 PSRs 2017). Such small PIs are unable to passport. The same applies to businesses qualifying and registered as small EMIs. See **Chapter 3 – Authorisation and registration and Chapter 6 – Passporting** for further information.

- Continue to exempt certain payment service providers (for example, banks) from authorisation/registration requirements

- Apply requirements to PIs regarding changes in qualifying holdings, so that the requirement, which already applied to EMIs, that individuals wishing to acquire or divest shares – whereby they pass a given threshold – are required to notify us. See **Chapter 4 – Changes in circumstances of authorisation and registration** for further information.

- Make changes to the appointment of agents and reflect that agents are required to be entered on an EBA register. See **Chapter 5 – Appointment of agents** for further information.

- Make changes to the conduct of business requirements. This means requirements for information to be provided to payment service users, and specific rules on the respective rights and obligations of payment service users and providers. See **Chapter 8 – Conduct of business requirements** for further information. In addition, banks and building societies need to comply with the Banking: Conduct of Business Sourcebook.

- Make changes to the requirements regarding safeguarding. See **Chapter 10 – Safeguarding** for further information.

- Make changes to the rules governing access to payment systems. The rules state that access should be non-discriminatory, subject to certain exemptions. This is aimed at supporting competition among payment service providers. **See** the Payment Systems Regulator's Approach Document for further information.

- Make changes to the rules governing the access to payment account services that credit institutions provide to other payment service providers. The rules state that access should be non-discriminatory. See **Chapter 16 – Access to payment account services** for further information.

- Introduce two new payment services: account information services (AIS) and payment initiation services (PIS) and sets out requirements and rights around when and how payment accounts can be accessed. Changes relating to these new payment services can be found throughout this document. See **Chapter 17 - Payment initiation and account information services and confirmation of available funds** for further information.

1.10. The PSRs 2017 required various changes to be made to this document and we recommend that businesses review all chapters that are relevant to them.

E-money

1.11. 2EMD was adopted by the European Parliament and the Council of the European Union in September 2009. The full text of 2EMD can be found on the European Commission's website.[1] 2EMD was transposed into UK law in April 2011, through the EMRs. The PSRs 2017 contain some consequential amendments to the EMRs.

1.12. EMIs are authorised or registered to issue e-money and undertake payment services under the EMRs, rather than under the Financial Services and Markets Act 2000 (FSMA). However, it should be noted that that issuing e-money remains a regulated activity under article 9B of the Regulated Activities Order 2001 for credit institutions (i.e. banks and building societies), credit unions and municipal banks, which means they will be authorised to issue e-money under a Part 4A FSMA permission.

1.13. Most e-money issuers are required to be either authorised or registered by us and to comply with rules about issuing e-money and carrying on payment services. The rules are set out in the EMRs, the PSRs 2017 and parts of the Handbook.

1.14. The EMRs set out:

- the definition of e-money and the persons that must be authorised or registered under the EMRs when they issue e-money
- standards that must be met by EMIs for authorisation or registration to be granted
- capital requirements and safeguarding requirements for EMIs
- rules on issuing and redeeming e-money for all e-money issuers
- our powers and functions in relation to supervision and enforcement in this area

1.15. The PSRs 2017 contain conduct of business rules that are applicable to most e-money issuers for the payment services part of their business.

---

1 Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (Text with EEA relevance).

1.16. Relevant to both payment services and e-money, the Handbook sets out, among other relevant material:

- the requirements for certain payment service providers and e-money issuers to submit returns
- complaints handling procedures that payment service providers and e-money issuers must have in place
- the right of certain customers to complain to the Financial Ombudsman Service (the ombudsman service)
- our policy and procedures for taking decisions relating to enforcement action and when setting penalties
- our ongoing fees
- levies for the ombudsman service and the Money Advice Service

1.17. Changes have been made to the Handbook following the implementation of PSD2, including to SUP reporting and PERG. We encourage businesses to carefully review the relevant sections.

Implementation dates and transitional provisions

1.18. The PSRs 2017 come into force for most purposes on 13 January 2018.

1.19. Prospective PIs and EMIs, applying under the PSRs 2017 and EMRs respectively (as amended to reflect PSD2), will be required to provide more information than under the current regime, including:

- procedures for incident reporting
- processes in place to file, monitor, track and restrict access to sensitive payment data
- principles and definitions applied for the collection of statistical data on performance, transactions and fraud
- arrangements for business continuity and procedure for testing and review of such plans
- a security policy document including a detailed risk assessment and mitigation measures taken to adequately protect payment service users against risks identified including fraud and illegal; use of sensitive and personal data.
- description of checks on agents and branches
- PII held (for businesses that propose providing AIS or PIS)

See **Chapter 3 – Authorisation and registration** and the relevant EBA guidelines and technical standards for more details.

1.20. The PSRs 2017 contain transitional provisions which will allow existing authorised PIs and EMIs to continue carrying on payment services activity without applying for authorisation under the regulations until 12 July 2018. If these businesses wish to continue with these services after this date they must provide us with the information set out above. This information must be submitted before 13 April 2018. There are separate provisions that apply to existing, authorised PIs and authorised EMIs that wish

to provide AIS and PIS. Please refer to **Chapter 3 – Authorisation and registration** for further information.

1.21. There are separate transitional provisions for existing small PIs and small EMIs. Small EMIs may carry on their activities without authorisation or registration until 12 July 2018, and small PIs until 12 January 2019. If they wish to continue providing such activity beyond these dates they will be required to re-apply to the FCA before 12 April 2018 and 12 October 2018 respectively, and provide any relevant information requested by the FCA.

1.22. Businesses should review the PSRs 2017, particularly Regulations 150 to 153 relating to transitional provisions.

Status of this document

1.23. The parts of this guidance that relate to payment services are given under regulation 120 of the PSRs 2017, while those that relate to EMIs are given under regulation 60 of the EMRs.

1.24. This is a 'live' document and may be updated as we receive feedback from businesses, trade associations and other stakeholders on additional issues they would like to see covered, or guidance that needs to be clarified. We will also update the document in the event of changes in the UK regulatory framework, including as a result of any negotiations following the UK's vote to leave the EU.

1.25. This document supports the legal requirements which are contained in the documents described below. It is essential to refer to the PSRs, the EMRs or relevant parts of the Handbook for a full understanding of the obligations imposed by the regime.

1.26. Guidance is not binding on those to whom the PSRs, EMRs and rules apply, nor does it have 'evidential' effect. It need not be followed in order to achieve compliance with the relevant regulation or other requirement. So, a payment service provider or e-money issuer cannot incur disciplinary liability merely because it has not followed guidance. Nor is there any presumption that departing from guidance indicates a breach of the relevant regulation.

1.27. Guidance is generally designed to throw light on a particular aspect of regulatory requirements, not to be an exhaustive description of businesses' obligations.

1.28. If a person acts in accordance with general guidance in the circumstances contemplated by that guidance, we will proceed as if that person has complied with the aspects of the requirement to which the guidance relates. For the reliance that can be placed on other guidance, see section 9.4 of the Supervision manual in the Handbook (Reliance on individual guidance).

1.29. DEPP 6.2.1G(4) in the Handbook sets out how we take into consideration guidance and other published materials when deciding to take enforcement action. Businesses should also refer to Chapter 2 of our Enforcement Guide for further information about the status of Handbook guidance and supporting materials.

1.30. Rights conferred on third parties (such as clients of a payment service provider or e-money issuer) cannot be affected by our guidance. Guidance on the PSRs, EMRs or other requirements represents our view, and does not bind the courts, for example in relation to an action for damages brought by a private person for breach of a regulation. A person may need to seek his or her own legal advice.

Key documents

1.31. Links are given in this document to the PSRs 2017, EMRs and relevant sections of the Handbook. Payment service providers and e-money issuers who are not authorised or certificated under the Financial Services and Markets Act 2000 (FSMA) will need to have particular regard to those parts of the Handbook that are set out in this document, but are not expressly subject to the rules in the other parts of the Handbooks for the purpose of payment services or e-money regulation. Payment service providers and e-money issuers should also review the FCA's Principles for Business (PRIN).

1.32. The requirements for payment services and e-money regulation, setting out the rules for the new regime, can be found in the following documents, which are all accessible on our website:

- **The Payment Services Regulations 2017**
- **The Electronic Money Regulations 2011**

The relevant parts of the FCA Handbook

1.33. The Handbook is an extensive document that sets out the rules and guidance for financial services regulation. A Reader's Guide to the Handbook is available on the Handbook website together with a User Guide for the online version. Most of the Handbook does not apply to EMIs (unless they are authorised under FSMA), PIs or to RAISPs. However, there are a few areas that contain relevant provisions. These are:

- Glossary
  This provides definitions of terms used elsewhere in the Handbook. Clicking on an italicised term in the Handbook will open up the glossary definition.

- General Provisions (GEN).

  GEN 2 contains provisions on interpreting the Handbook.

- Banking: Conduct of Business sourcebook (BCOBS).

  Retail deposit takers (including banks and building societies) are also required to comply with the conduct of business rules for retail banking contained in BCOBS. BCOBS Chapter 1 contains further detail on which provisions are complementary to the PSRs and which provisions of do not apply to accounts where Parts 6 and 7 of the PSRs apply.

- Consumer Credit sourcebook (CONC)

This is the specialist sourcebook for credit-related regulated activities and contains detailed obligations that are specific to credit-related regulated activities and activities connected to those credit-related regulated activities. If [payment service providers] are involved in such activities, they will need to comply with CONC in addition to other requirements which are imposed by the Consumer Credit Act 1974 and legislation made under it.

- Fees manual (FEES).
  This contains fees provisions for funding the FCA and the FOS relevant to payment service providers.

- Supervision manual (SUP)

  SUP 5.3 and SUP 5.4 describe our policy on the use of skilled persons to carry out reports (see **Chapter 12 – Supervision** for further information)

  SUP 9 describes how people can seek individual guidance on regulatory requirements and the reliance they can place on guidance received

  SUP 11.3 and SUP 11 Annex 6G provide guidance on Part 12 of FSMA, relating to control over authorised EMIs and authorised PIs

  SUP 15.14 [new] sets out the notification requirements under the PSRs 2017

  SUP 16.13 sets out the forms, content, reporting periods and due dates for the reporting requirements under the PSRs 2017 (including annual returns)

  SUP 16.15 sets out the forms, content, reporting period and due dates for the reporting requirements under the EMRs

- Decision procedure and penalties manual (DEPP).
  This contains the procedures we must follow for taking decisions in relation to enforcement action and setting penalties.

- Dispute resolution: complaints sourcebook (DISP).
  This contains the obligations on payment service providers and e-money issuers for their own complaint handling procedures and complaints reporting. It also sets out the rules concerning customers' rights to complain to the FOS.

1.34. The Handbook website also contains the following regulatory guides that are relevant to payment service providers:

- Enforcement guide (EG).
  This describes our approach to exercising the main enforcement powers given to us under FSMA and the PSRs 2017.

- Financial Crime: a guide for firms (FC).
  This contains guidance on the steps businesses can take to reduce their financial crime risk.

- Perimeter guidance manual (PERG) – PERG 3A and PERG 15.
  This contains guidance aimed at helping businesses consider whether they need to be separately authorised or registered for the purposes of providing payment services in the UK.

- Unfair contract terms and consumer notices regulatory guide (UNFCOG).
  This guide explains our powers under the Unfair Terms in Consumer Contracts Regulations 1999 and our approach to exercising them.

1.35. There is also guidance and information issued by us, the FOS and HMRC which is likely to be relevant to readers of this document. This is referenced in the appropriate section of the document and gathered together in **Annex 1 - Useful links.**

Contacting us

1.36. We hope this document will answer all your questions; however, if you have any comments regarding this document or any aspect of the PSRs 2017 or EMRs, please refer to the contacts page on our website.

1.37. **Annex 2** contains a list of other useful contact details.

2. Scope

2.1 Part I of this chapter sets out who and what is covered by the PSRs 2017. Part II sets out who and what is covered by the EMRs, including what e-money is and information about e-money issuers. Each section sets out where to find further information on scope issues.

Part I: PSRs 2017

Who the PSRs 2017 cover

2.2 The PSRs 2017 apply, with certain exceptions, to everyone who provides payment services as a regular occupation or business activity in the UK ('payment service providers' (PSPs)). They also apply in a limited way to persons that are not payment service providers (see regulations 38, 39, 57, 58 and 61).

2.3 Chapter 15 of our Perimeter Guidance (PERG 15) gives guidance for firms who are unsure whether their activities fall within the scope of the PSRs 2017.

2.4 For a fuller understanding of the scope of the PSRs 2017, the guidance should be read in conjunction with Schedule 1 of the PSRs 2017 and the definitions in regulation 2.

Payment institutions

2.5 The PSRs 2017 establish a class of firms authorised or registered to provide payment services called payment institutions (PIs).

2.6 We expect that the following types of firms will require authorisation or registration for their payment services activities, amongst others:

- money remitters
- certain electronic communication network operators (offering payment services)
- non-bank credit card issuers
- merchant acquiring firms
- payment initiation service providers
- account information service providers

2.7 Not all providers of payment services require authorisation or registration under the PSRs 2017 (see 'Other payment service providers' below).

2.8 A payment service provider authorised under the PSRs 2017 is termed an 'authorised PI' and receives the right to 'passport' that authorisation to other EEA member states (see **Chapter 6 – Passporting**).

2.9 Payment service providers who meet the criteria for registration under regulation 14, and choose to apply for registration rather than authorisation, are referred to as small PIs. Small PIs cannot provide AIS or PIS.

2.10 **Chapter 3 – Authorisation and registration** gives details of the procedures for authorisation and registration.

2.11 All PIs (and most other PSPs) must comply with the conduct of business requirements of the PSRs 2017, described in **Chapter 8 – Conduct of business requirements.**

RAISPs

2.12 Businesses that only provide AIS are exempt from full authorisation but are subject to a registration requirement. Once registered, they are termed 'registered account information service providers' and can 'passport' into other EEA member states.

2.13 RAISPs are only required to comply with specific parts of the conduct of business requirements. These are identified in paragraphs 8.132 to 8.136 of **Chapter 8 – Conduct of business requirements**.

Agents

2.14 PIs may provide payment services through agents, subject to prior registration of the agent with us. **Chapter 5 – Appointment of agents** gives details of the process to be followed.

2.15 It is the PI's responsibility to ensure the agent complies with the conduct of business requirements of the PSRs 2017 and that it has the systems and controls in place to effectively oversee their activities.

Other payment service providers

2.16 The following can provide payment services without the need for further authorisation or registration by the FCA under the PSRs 2017:

- banks
- building societies
- EEA authorised PIs
- EEA RAISPs
- authorised EMIs
- small EMIs
- EEA authorised EMIs
- Post Office Limited
- certain public bodies

These entities must, however, comply with the conduct of business requirements of the PSRs 2017 described in **Chapter 8 – Conduct of business requirements**.

2.17 In the case of credit institutions, the relevant application or certification procedures remain those in FSMA. Credit institutions are also subject to the FCA rules and guidance in the FCA Banking: Conduct of Business Sourcebook (BCOBS) – see **Chapter 8 – Conduct of business requirements**.

2.18 For EMIs, the relevant application procedures are those in the EMRs, which also contain conduct of business provisions in relation to the issuance and redemption of e-money (see **Chapter 8 – Conduct of business requirements**).

2.19 Credit institutions will need to notify us if they wish to provide the new payment services of account information and payment initiation, and existing EMIs will need to apply to remove the requirement on their permission imposed by regulation 78A of the EMRs, see **Chapter 3 – Authorisation and registration**, and **Chapter 13 – Reporting and Notifications.**

Exemptions

2.20 The following bodies are specifically exempt from the scope of the PSRs 2017:

- credit unions
- municipal banks
- The National Savings Bank

2.21 Municipal banks and the National Savings Bank are also exempt from BCOBS. Municipal banks must nevertheless notify us if they are providing, or propose to provide, payment services. Credit unions are subject to BCOBS.

Exclusions

2.22 More generally, there is a broad range of activities which do not constitute payment services under Schedule 1 Part 2 to the PSRs 2017. Amongst these excluded activities, are:

- payment transactions through commercial agents acting on behalf of either the payer or the payee;
- cash to cash currency exchange activities (for example, bureaux de change);
- payment transactions linked to securities asset servicing (for example, dividend payments, share sales or unit redemptions);
- services provided by technical service providers (which does not include AIS or PIS).
- payment services based on instruments used within a limited network of service providers or for a very limited range of goods or services ("limited network exclusion"); and
- payment transactions for certain goods or services up to certain value limits, initiated through a provider of electronic communication networks or services ("electronic communications network exclusion")

2.23 Chapters 3A and 15 of PERG provide more information on these exclusions.

Registers

2.24 The Financial Services Register, published on our website includes information relating to various types of payment service provider, together with details of the payment services that they are entitled to provide. The register includes details relating to:

- authorised PIs and EMIs, their EEA branches and their agents
- small PIs and EMIs and their agents
- RAISPs and their agents
- persons providing a service falling within the limited network exclusion or the electronic communications exclusion who have notified us in line with regulation 38 or 39 of the PSRs 2017

- credit unions, municipal banks and the National Savings Banks, where they provide payment services

2.25 The EBA will also maintain a register which includes the information covered in our public register, together with information provided by the competent authorities in other EEA Member States. This will be available free of charge on the EBA's website.

Payment services

2.26 The payment services covered by the PSRs 2017 (Part 1 of Schedule 1) are set out in the table below, along with some examples of the sort of payment services expected to fall within their scope. The table is high-level and indicative in nature. If firms are in any doubt as to whether their activities constitute payment services, they should refer to Chapter 15 of our Perimeter Guidance manual ("PERG").

2.27 In addition to questions and answers providing further information on payment services, PERG also explains a number of exclusions in the PSRs 2017. These exclusions are set out in Part 2 of Schedule 1 to the PSRs 2017 (Activities which do not constitute payment services). For businesses that intend to rely on paragraphs 2(k) or 2(l) of Part 2 of Schedule 1 to the PSRs 2017 (i.e. the limited network exclusion or the electronic communication network exclusion), certain notification requirements apply. See **Chapter 13 – Reporting and Notifications.**

What is a payment service?	**Examples (PERG 15 provides further details about what activities constitute payment services)**
Services enabling cash to be placed on a payment account and all of the operations required for operating a payment account.	• payments of cash into a payment account over the counter and through an ATM
Services enabling cash withdrawals from a payment account and all of the operations required for operating a payment account.	• withdrawals of cash from payment accounts, for example through an ATM or over the counter
Execution of the following types of payment transaction: • direct debits, including one-off direct debits • payment transactions executed through a payment card or a similar device • credit transfers, including standing orders	• transfers of funds with the customer's payment service provider or with another payment service provider • direct debits (including one-off direct debits). However, acting as a direct debit originator would not, of itself, constitute the provision of a payment service. • debit card payments • transferring e-money • credit transfers, such as standing orders, Faster Payments, BACS or CHAPS payments
Execution of the following types of payment transaction where the funds are covered by a credit line for a payment service user: • direct debits, including one-off direct debits • payment transactions through a payment card or a similar device • credit transfers, including standing orders	• direct debits using overdraft facilities • credit card payments • debit card payments using overdraft facilities • credit transfers using overdraft facilities
Issuing payment instruments or acquiring of payment transactions.	• card issuing including where the card issuer provides a card linked to an account held with a different payment service provider (see regulation 68 of the PSRs 2017) but not including mere technical service providers who do not come into possession of funds being transferred • merchant acquiring services (rather than merchants themselves)
Money remittance.	• money transfer/remittances that do not involve creation of payment accounts.
Payment initiation services.	• services provided by businesses that contract with online merchants to enable customers to purchase goods or services through their online banking facilities, instead of using a payment instrument or other payment method.

Account information services.	• businesses that provide users with an electronic "dashboard" where they can view information from various payment accounts in a single place • businesses that use account data to provide users with personalised comparison services • businesses that, on a user's instruction, provide information from the user's various payment accounts to both the user and third party service providers such as financial advisors or credit reference agencies

Scope of the PSRs 2017: jurisdiction and currency

2.25 The table below shows the jurisdictional scope of different parts of the PSRs 2017 and their scope in terms of the currency of the payment transaction.

2.26 The 'corporate opt-out' may apply to certain of the conduct of business provisions – see Part 1 of **Chapter 8 – Conduct of business requirements** for further details.

2.27 Where we refer to 'one leg transactions' below, we mean those where either the payer's or the payee's payment service provider (rather than the payer or payee) is located outside the EEA. Where we refer to 'intra EEA', we mean those where both the payer's and the payee's payment service providers are (or the sole payment service provider is) located in the EEA.

Payment services – jurisdictional and currency scope		
PSRs 2017	**Jurisdiction**	**Currency**
Authorisation/Registration (including meeting capital and safeguarding requirements).	Firms providing payment services, as a regular occupation or business activity in the UK including one leg out transactions, unless the firm is in the list of 'other payment service providers' described above.	All currencies.
Complaints that can be considered by the FOS (see Chapter 11 for full details of eligibility).	All payment services provided from a UK establishment, including the UK end of one leg out transactions.	All currencies.
Part 6 - Conduct of business requirements (information requirements)	In general, Part 6 applies to payment services provided from a UK establishment including the UK end of one leg out and intra EEA transactions, in any currency. For one leg out transactions, Part 6 only applies in respect of those parts of a transaction that are carried out in the EEA. We set out other exceptions to this in a separate table below.	
Part 7 – Conduct of business requirements (rights and obligations in relation to the provision of payment services)	In general, Part 7 applies to payment services provided from a UK establishment including the UK end of one leg and intra EEA transactions, in any currency. For one leg transactions, Part 7 only applies in respect of those parts of a transaction that are carried out in the EEA. We set out below other exceptions to this in a separate table.	

Part 6 – Exceptions to where Part 6 applies to one and two leg transactions in any currency. Does the regulation apply?				
PSRs 2017	**One leg / EEA currency**	**One leg / non EEA currency**	**Intra EEA/ EEA currency**	**Intra EEA/ non-EEA currency**
Regulation 43(2)(b) – Pre-contractual information about execution times for single payment contracts	No	No	Yes	No
Regulation 52(a) – Information about execution times prior to execution of individual transactions under a framework contract	No	No	Yes	No
Paragraph 2(e) of Schedule 4 – Pre-contractual information about execution times for framework contracts	No	No	Yes	No
Paragraph 5(g) of Schedule 4 – Pre-contractual information about the conditions for the payment of any refund under regulation 79.	No	No	Yes	Yes

Part 7 – Exceptions to where Part 7 applies to one and two leg transactions in any currency. Does the regulation apply?				
PSRs 2017	**One leg / EEA currency**	**One leg / non EEA currency**	**Intra EEA EEA currency**	**Intra EEA/ non-EEA currency**
Regulation 66(2) – charges paid by payer and payee	No	No	Yes	Yes
Regulation 79 – Refunds for transactions initiated by or through a payee	No	No	Yes	Yes
Regulation 80 – Requests for refunds for transactions initiated by or through a payee	No	No	Yes	Yes
Regulation 84 – Amounts transferred and received	No	No	Yes	No

Regulation 85 – Application of Regulations 86 – 88	Yes	Yes	Yes	No
Regulation 86(1)-(3) - Payment transactions to a payment account	No*	No*	Yes (subject to regulation 85)	No*
Regulation 86(4)-(5) - Payment transactions to a payment account	Yes (subject to regulation 85)	Yes (subject to regulation 85)	Yes (subject to regulation 85)	No
Regulation 87 – Absence of payee's payment account with payment service provider	Yes (subject to regulation 85)	Yes (subject to regulation 85)	Yes (subject to regulation 85)	No
Regulation 88 – Cash placed on a payment account	Yes (subject to regulation 85)	Yes (subject to regulation 85)	Yes (subject to regulation 85)	No
Regulation 91 – non-execution or late execution of payment transaction initiated by the payer	No	No	Yes	Yes
Regulation 92 – non-execution or late execution of payment transaction initiated by the payee	No	No	Yes	Yes
Regulation 94 – Liability of service providers for charges and interest	No	No	Yes	Yes
Regulation 95 – right of recourse	No	No	Yes	Yes

* This means that when making transactions to a payment account the time limits for crediting a payee's payment service provider's account will not apply to one leg in transactions for transactions in non-EEA currencies.

Part II: EMRs

Who the EMRs cover

2.28 The EMRs apply, with certain exceptions, to everyone who issues e-money in the UK. They also apply in a limited way to persons that are not e-money issuers (see regulations 32).

2.29 Chapter 3a of our Perimeter Guidance (PERG 3A) gives guidance for firms who are unsure whether their activities fall within the scope of the EMRs.

2.30 For a fuller understanding of the scope of the EMRs this guidance should be read in conjunction with the definitions in regulation 2 of the EMRs.

How e-money is defined

2.31 Regulation 2 of the EMRs defines e-money as monetary value represented by a claim on the issuer that is:

- stored electronically, including magnetically
- issued on receipt of funds for the purpose of making payment transactions (see regulation 2 of the PSRs 2017)
- accepted as a means of payment by persons other than the issuer
- is not excluded by regulation 3 of the EMRs (see paragraphs 2.36 below)

2.32 Examples of e-money include prepaid cards that can be used to pay for goods at a range of retailers, or virtual purses that can be used to pay for goods or services online.

Exclusions

2.33 There are two express exclusions in Regulation 3 of the EMRs. Chapters 3A and 15 of PERG provide more information on these exclusions. The exclusions mirror paragraphs 2(k) and 2(l) of Part 2 of Schedule 1 to the PSRs 2017 (i.e. the limited network exclusion and the electronic communication network exclusion).

How the EMRs define e-money

2.34 E-money issuers are defined in the EMRs as any of the following persons when they issue e-money:

EMIs:

2.35 The EMRs establish a class of firms authorised or registered to issue e-money and provide payment services called EMIs.

2.36 Not all issuers of e-money require authorisation or registration under the EMRs (see other e-money issuers below).

2.37 An EMI which receives authorisation under the EMRs is termed an 'authorised EMI' and receives the right to 'passport' that authorisation to other EEA member states (**see Chapter 6 – Passporting**).

2.38 EMIs that meet the criteria for registration under regulation 12 EMRs, and choose to apply for registration rather than authorisation, are referred to as 'small EMIs'.

Chapter 3 – Authorisation and registration gives details of the procedures for authorisation and registration.

2.39 All EMIs must comply with the conduct of business requirements of the PSRs 2017 and EMRs described in **Chapter 8 – Conduct of business requirements**.

European Economic Area (EEA) authorised EMIs:

2.40 Persons authorised in an EEA state other than the UK to issue e-money and provide payment services in accordance with 2EMD Persons authorised in other EEA states to issue e-money and provide payment services may exercise passport rights to issue, distribute or redeem e-money or provide payment services in the UK in accordance with 2EMD. The competent authority of the home state is responsible for prudential regulation and, where passporting is on an establishment basis rather than a cross-border service provision basis, we (as the host state competent authority) will be responsible for conduct of business regulation (see **Chapter 6 - Passporting**) and anti-money laundering supervision (see **Chapter 19 – Financial Crime**).

E-money issuers who require Part 4A permission under FSMA:

2.41 Credit institutions, credit unions and municipal banks do not require authorisation or registration under the EMRs but if they propose to issue e-money they must have Part 4A permission under FSMA for the activity of issuing e-money. When issuing e-money, they are subject to the provisions on issuance and redeemability of e-money in the EMRs (see **Chapter 8 – Conduct of business requirements**). In addition credit unions are subject to the safeguarding requirements (see **Chapter 10 - Safeguarding**).

Other e-money issuers

2.42 The following can issue e-money and do not need to apply for authorisation or registration under the EMRs but they must give us notice if they issue or propose to issue e-money:

- Post Office Limited;
- the Bank of England, the European Central Bank and the national central banks of EEA states other than the UK, when not acting in their capacity as a monetary authority or other public authority;
- government departments and local authorities when acting in their capacity as public authorities; and
- the National Savings Bank.

2.43 They will be subject to the conduct of business requirements of the EMRs, the conduct of business requirements of the PSRs 2017 for the payment service aspect, and they will have to report to us their average outstanding e-money on a yearly basis. Certain customers will have access to the Ombudsman Service.

2.44 PERG 3A gives guidance for businesses that are unsure whether their activities fall within the scope of the EMRs.

Use of Agents and Distributors

2.45 EMIs may distribute and redeem e-money and provide payment services through agents, subject to prior registration of the agent by us. **Chapter 5 – Appointment of agents** gives details of the process to be followed.

2.46 EMIs may engage distributors to distribute and redeem e-money. An EMI cannot provide payment services through a distributor, and distributors do not have to be registered by us but applicants will have to identify their proposed use of distributors and, where they intend to distribute e-money in another EEA states by engaging distributors, EMIs will need to provide details of distributors in their passporting notification (see **Chapter 6 - Passporting**).

EMIs providing payment services

2.47 All EMIs may provide payment services, including those that are not related to the issuing of e-money (unrelated payment services). EMIs must, however, tell us about the types of payment services they wish to provide (see **Chapter 3 – Authorisation and Registration**).

2.48 Small EMIs can only provide unrelated payment services if the average monthly total of payment transactions does not exceed €3m on a rolling 12-month basis (see **Chapter 3 – Authorisation and registration**).

EMIs providing AIS and PIS

2.49 Regulation 78A of the EMRs has the effect of placing a requirement on EMIs authorised before 13 January 2018 preventing them from providing AIS or PIS. Authorised EMIs will need to apply to us if they wish to have this requirement removed - see **Chapter 3 – Authorisation and Registration**. Small EMIs cannot provide AIS or PIS.

3. Authorisation and registration

3.1 This chapter sets out how we will apply the PSRs 2017 and EMRs dealing with:

- authorisation of PIs and EMIs (Part I)
- registration of small PIs and small EMIs (Part II)
- registration of businesses only providing AIS (Part III)
- decision-making process (Part IV)
- transitional provisions (Part V)

3.2 For information on notifications relating to exclusions please see **Chapter 13 – Reporting and notifications**.

Introduction

3.3 A UK business that provides payment services (as defined in the PSRs 2017) as a regular occupation or business activity in the UK needs to apply to us to become either an authorised PI, a small PI or a RAISP, unless it is already another type of payment service provider or is exempt.

3.4 Being a small PI is an option available to businesses with average payment transactions turnover that does not exceed €3 million per month and who do not provide AIS or payment initiation services (PIS). The registration process is cheaper and simpler than authorisation and has no ongoing capital requirements, but there are no passporting rights for small PIs. The conduct of business requirements still apply, as does access for small PIs' eligible customers to the Ombudsman Service.

3.5 A UK business (or a UK branch of a business with its head office outside the EEA) that intends to issue e-money needs to apply to us to become either an authorised EMI or a small EMI, unless it has permission under Part 4A FSMA to issue e-money or is exempt. Being a small EMI is an option available to businesses whose total business activities are projected to generate average outstanding e-money that does not exceed €5 million.

3.6 In accordance with regulation 32 of the EMRs, EMIs are allowed to provide payment services without being separately authorised under the PSRs 2017. This includes payment services that are unrelated to the issuance of e-money. If a small EMI provides payment services unrelated to the issuance of e-money this is on the same basis as a small PI; that is, the monthly average, over a period of 12 months, of the total amount of relevant payment transactions must not exceed €3 million. Regulation 78A of the EMRs has the effect of placing a requirement on EMIs authorised before 13 January 2018 preventing them from providing AIS or PIS. Authorised EMIs will need to apply to us to have this requirement removed - see Chapter 3 – Authorisation and Registration. Small EMIs cannot provide AIS or PIS.

3.7 Agents can be appointed by a PI/EMI (the principal) to provide payment services on the principal's behalf. The principal accepts responsibility for the actions of the agent and

must apply for the agent to be registered on the Financial Services Register. More information on agents is contained in **Chapter 5 – Appointment of agents**.

3.8 EMIs may also engage distributors to distribute and redeem e-money. A distributor cannot provide payment services, and does not have to be registered by us – but applicants will have to identify their proposed use of distributors at authorisation and, where they engage distributors to distribute or redeem e-money in other EEA states, provide their details in passporting notifications (see **Chapter 6 - Passporting**).

3.9 The FCA's Financial Services Register is a public record of firms, individuals and other bodies that are, or have been, regulated by the PRA and/or FCA. The Register contains information about PIs, RAISPs, EMIs, agents and EEA branches. See Part III of this document for more information on RAISPs. The EBA will maintain a register which includes the information covered in our public register, together with information provided by the competent authorities in other EEA Member States. This will be available free of charge on the EBA's website.

3.10 Anyone wishing to become authorised or registered needs to complete an application form and submit it to us along with the required information and the application fee (see below – fees will vary depending on the application).

3.11 Application forms are available after registering on Connect. No work will be done on processing the application until the full fee is received. The fee is non-refundable and must be paid via Connect. Application forms for applicants wishing to become authorised EMIs are available on the e-money section of our website. The fee must be paid by cheque.

3.12 Applicants that wish to operate through agents will be charged an additional application fee. See **Chapter 15 – Fees** for more information.

3.13 The EBA has issued "Guidelines on the information to be provided for authorisation as payment institutions and e-money institutions and registration as account information service providers" (EBA Guidelines).[2] The guidelines specify the information that applicants for authorisation or registration as a RAISP will be required to submit. Details on these requirements are set out below in Part 1. In some cases we will also apply relevant guidelines when specifying the information to be provided by applicants for registration as small PIs or small EMIs. More detail on these requirements is set out in Part II.

3.14 Where we do not prescribe the format of information you give us, we will need to have enough information to be satisfied that you meet the relevant conditions. This does not mean that you need to enclose full copies of all the procedures and manuals with the applications; a summary of what they cover may be enough, as long as the manuals and procedures themselves are available if we want to investigate further. Note that supplying the information requested on the application form will not necessarily be enough for the application to be 'complete'. We may need to ask additional questions or request additional documentation to clarify the answers already given. It is only

[2] Available at https://www.eba.europa.eu/-/eba-consults-on-guidelines-on-authorisation-and-registration-under-psd2

when this additional information has been received and considered alongside the existing information that we will be able to determine whether the application is complete.

3.15 We will acknowledge that we have received your application within seven days of receiving it, and the case officer assigned to deal with it will be in contact soon after. We will assess the information you provide against the requirements set out in the PSRs 2017, EMRs and the EBA Guidelines (where applicable). Where applications are incomplete (when they do not have all the information we need), we will ask you in writing for more information. We will let you know the date when we consider the application to be complete. The timings set out in Part IV: Decision-making process will run from that date.

3.16 Applicants should note that under regulation 114 of the PSRs 2017 and regulation 66 of the EMRs it is a criminal offence to deliberately or recklessly give misleading information in the application.

Requests for further information (regulations 5(4) 13(4) and 17(2) PSRs 2017 and 5(4) and 12(4) EMRs)

3.17 At any time after receiving an application for authorisation or registration (or a variation of either of these) and before determining it, we can require the applicant to provide such further information as we reasonably consider necessary to enable us to determine the application. Where an application is incomplete, firms will need to provide information promptly to avoid delay to consideration of their application (see 'Timing' in Part IV of this chapter).

Duty to advise of material changes in an application (regulation 20 PSRs 2017 and 17 EMRs)

3.18 We attach considerable importance to the completeness and accuracy of the information provided to us. If there is, or is likely to be, any material change in the information provided for an application before we have made our decision on it, the applicant must notify us. This also applies if it becomes apparent to the applicant that there is incorrect or incomplete information in the application. The requirements also apply to changes to supplementary information already provided. If an applicant fails to provide accurate and complete information it will take longer to assess the application. In some cases, it could lead to the application being rejected.

3.19 The notification must include details of the change, the complete information or a correction of the inaccuracy (as the case may be) and must be made without undue delay. If the applicant expects a change in the future they must provide details as soon as they become aware of it. When providing this information the applicant will be asked to confirm that the rest of the information in the application remains true, accurate and complete.

3.20 Applicants should notify the case officer assigned to the application (the case officer will be in contact with an applicant after receipt of the application).

Part I: Becoming an authorised PI or authorised EMI

3.21 This section applies to businesses that wish to become an authorised PI or an authorised EMI.

3.22 The conditions that must be met in order to become an authorised PI are set out in regulation 6 of the PSRs 2017 and those that must be met to become an authorised EMIs are set out in regulation 6 of the EMRs.

3.23 The information requirements for your application can be found in Schedule 2 to the PSRs 2017 and section 4.1 of the EBA Guidelines (the API Guidelines) for PIs and Schedule 1 to the EMRs and section 4.3 of the EBA Guidelines (the EMI Guidelines) for EMIs.

3.24 The application fees to become an authorised PI or an authorised EMI are set out in **Chapter 15 – Fees**.

3.25 For authorised PIs and EMIs, the application must be signed by the person(s) responsible for making the application on behalf of the applicant firm. The appropriate person(s) depends on the applicant firm's type as follows:

Type of applicant	**Appropriate signatory**
Company with one director	The director
Company with more than one director	Two directors
Limited liability partnership	Two members
Limited partnership	The general partner or partners

Information to be provided and conditions for authorisation

3.26 Authorisation will not be granted unless we are satisfied in that the conditions specified in regulation 6 of the PSRs 2017 or EMRs (as the case may be) have been met.

3.27 This section needs to be read alongside Chapter 4.1 of the EBA Guidelines (the API Guidelines) or Chapter 4.3 of the EBA Guidelines (the EMI Guidelines), as appropriate. Together, the PSRs 2017 and the API Guidelines, and the EMRs and the EMI Guidelines explain the information that you must supply with the application and the conditions that must be satisfied.

Programme of operations (Paragraph 1, Schedule 2 PSRs 2017 and Paragraph 1, Schedule 1 EMRs)

3.28 For PIs, API Guideline 3 sets out the information and documentation which needs to be provided for the programme of operations. For EMIs this is set out in EMI Guideline 3.

3.29 In both cases Guideline 3 requires the programme of operations to be provided by the applicant to contain a description of the payment services envisaged, including an explanation on how the activities and the operations fit into the list of payment services set out in Part 1 of Schedule 1 to the PSRs 2017. Some examples of the sorts of activities expected to fall within the scope of each are described in **Chapter 2 - Scope**, with further guidance in Chapter 15 of our Perimeter Guidance Manual (PERG).

3.30 The applicant is also required to state whether they will enter into the possession of users' funds. In our view being in possession of funds includes an entitlement to funds in a bank account in your name, funds in an account in your name at another PI and funds held on trust for you.

Business plan (regulation 6(7)(c) and paragraph 2, Schedule 2 PSRs 2017 and regulation 6(6)(c) and paragraph 2, Schedule 1 EMRs)

3.31 API Guideline 4 and EMI Guideline 4 set out the information and documentation which needs to be provided in the business plan.

3.32 The business plan needs to explain how the applicant intends to carry out its business. It should provide enough detail to show that the proposal has been carefully thought out and that the adequacy of financial and non-financial resources has been considered.

3.33 In accordance with regulation 7(4) of the PSRs 2017 and regulation 7(4) of the EMRs, where an applicant wishes to carry out business activities other than the provision of payment services and, in the case of EMIs, issuing e-money and we think that the carrying on of this business will, or is likely to, impair our ability to supervise it or its financial soundness, we can require the applicant to form a separate legal entity to provide payment services and, for EMIs, issue e-money.

3.34 Applicants wishing to become authorised EMIs that intend to provide unrelated payment services are required to submit a separate business plan for these activities.

Initial capital (regulation 6(3) and paragraph 3, Schedule 2 PSRs 2017 and regulation 6(3) and paragraph 3, Schedule 1 EMRs)

3.35 Applicants are required to provide information on their own funds, including the amount and detailed breakdown by paid-up capital, reserves and retained earnings as part of their business plan (see API Guideline 4 and EMI Guideline 4). By the time of authorisation, the applicant must provide evidence that they hold initial capital at the level required by Part 1 of Schedule 3 to the PSRs 2017 or Part 1 of Schedule 2 to the EMRs as the case may be. API Guideline 6 and EMI Guideline 6 sets out the information and documentation to be provided as evidence of initial capital.

3.36 The initial capital requirement for authorised EMIs is €350,000. Applicants wishing to become authorised EMIs that intend to provide unrelated payment services should note that there is no additional initial capital requirement.

3.37 For applicants to become authorised PIs the level of initial capital required depends on the payment services to be provided, and is the greater of the following:

Payment services **(see Schedule 1 to the PSRs 2017)**	**Initial capital required**
AIS (paragraph 1(h), Schedule 1 to the PSRs 2017)	None
Money remittance (paragraph 1(f) of Part 1, Schedule 1 to the PSRs 2017)	€20,000
PIS (paragraph 1(g) of Part 1, Schedule 1 to the PSRs 2017)	€50,000
Payment institutions providing services in Schedule 1 Part 1(1)(a) to (1)(e) to the PSRs 2017.	€125,000

3.38 The evidence needed will depend on the type of firm and its source of funding. For example, if an applicant was a limited company and using paid-up share capital, we would expect to see a copy of the SH01 form submitted to Companies House and a bank statement, in the business name, showing the monies being paid in. If an applicant has already been trading and has sufficient reserves to meet the initial capital requirement, then a copy of the audited last year-end accounts may be enough (or interim accounts if appropriate). Businesses may wish to capitalise nearer to the time of authorisation, so this evidence can be provided at a later date but will be required before authorisation is granted.

Safeguarding measures (regulation 6(7)(d) and paragraph 4, Schedule 2, PSRs 2017 and regulation 6(6)(d) and paragraph 4, Schedule 1 EMRs)

3.39 Applicants are required to satisfy the FCA that they have taken adequate measures for the purpose of safeguarding user's funds. For applicants to become authorised EMIs that intend to provide unrelated payment services this includes the safeguarding measures they intend to use to satisfy regulation 23 of the PSRs 2017, as modified by regulation 20(6) of the EMRs in respect of those funds. API Guideline 7 and EMI Guideline 7 set out the information and documentation which needs to be provided in relation to safeguarding.

3.40 There is more information in **Chapter 10 – Safeguarding** on safeguarding measures including guidance on what we would expect to see by way of organisational arrangements.

3.41 This requirement does not apply to applicants that will not receive funds from or on behalf of payment service users, or in exchange for e-money, such as those that intend only to provide PIS and AIS. See **Chapter 10 – Safeguarding** for more information on this.

Professional Indemnity insurance (PII) (regulation 6(7)(e) and (f)) and paragraph 19, Schedule 2 PSRs 2017 and regulation 6(6)(e) and (f) and paragraph 14 EMRs

3.42 Where an applicant for authorisation as a PI seeks permission to provide PIS or AIS it must satisfy the FCA that it holds appropriate professional indemnity insurance or a comparable guarantee.

3.43 Authorised EMIs who intend to provide either PIS or AIS will also need to hold the required PII. If the applicant does not intend to provide these services it must state so in its application. In these cases authorisation will be subject to a requirement under regulation 7 EMRs that the applicant will not undertake these activities.

3.44 API Guideline 18 and EMI Guideline 18 sets out the information and documentation that is required for this insurance or guarantee.

Governance arrangements, internal controls and risk management (regulation 6(6) and paragraphs 5 to 11 Schedule 2, PSRs 2017 and regulation 6(5) and paragraphs 5 to 6 Schedule 1 the EMRs)

3.45 Applicants must satisfy the FCA that their governance arrangements, internal control mechanisms and risk management procedures meet the conditions set out in regulation 6(6) PSRs 2017 or regulation 6(5) EMRs.

3.46 We will assess if the arrangements, controls and procedures are appropriate, sound and adequate taking account of a number of factors, such as the:

- payment services being provided
- nature, scale and complexity of its business
- diversity of its operations, including geographical diversity
- volume and size of its transactions
- degree of risk associated with each area of its operation

3.47 Paragraphs 5 to 12 of Schedule 2 to the PSRs 2017, and paragraphs 5 to 7 of Schedule 1 to the EMRs set out information requirements that are relevant to these conditions, and more detail is provided by the Guidelines.

Governance arrangements, risk management and internal controls (paragraph 5 Schedule 2 PSRs 2017 and paragraph 5 Schedule 1 EMRs)

3.48 API Guideline 8 and EMI Guideline 8 sets out the information and documentation that needs to be provided for governance arrangements, risk management and internal controls.

3.49 Governance arrangements are the procedures used in decision-making and control of the business that provide its structure, direction and accountability.

3.50 The description of the risk management procedures provided in the application should show how the business will effectively identify, manage, monitor and report any risks to which the applicant might be exposed.

3.51 A map of the risks identified by the applicant, including the types of risks and the procedures the applicant will put in place to assess and prevent such risks should be provided. Such risks may include:

- settlement risk (a settlement of a payment transaction does not take place as expected)
- operational risk (loss from inadequate or failed internal processes, people or systems)
- counterparty risk (that the other party to a transaction does not fulfil its obligations)
- liquidity risk (inadequate cash flow to meet financial obligations)
- market risk (risk resulting from movement in market prices)
- financial crime risk (the risk that the PI or its services might be used for a purpose connected with financial crime)
- foreign exchange risk (fluctuations in exchange rates)

3.52 Depending on the nature and scale of the business and the payment services being undertaken, it may be appropriate for the PI to operate an independent risk management function. Where this is not appropriate, the PI should be able to demonstrate that the risk management policies and procedures it has adopted are effective.

3.53 Internal controls are the systems, procedures and policies used to safeguard the business from fraud and error, and to ensure accurate financial information. They should include sound administrative and accounting procedures so the applicant can give us financial reports that reflect a true and fair view of its financial position and that will allow them to comply with the requirements of the PSRs 2017 in relation to its customers.

3.54 Our assessment of the application will consider if the systems and controls described in the information supplied are adequate and appropriate to the payment services activities that the applicant intends to carry on.

Security incidents and security-related customer complaints (paragraph 6 Schedule 1 PSRs 2017 and paragraph 5A Schedule 2 EMRs)

3.55 API Guideline 9 and EMI Guideline 9 set out the information and documentation required for security incidents and security-related customer complaints. The information required included details of how the applicant will comply with its obligation to report major operational or security incidents under regulation 99 PSRs 2017.

Sensitive payment data (paragraph 7 Schedule 1 PSRs 2017 and paragraph 5B Schedule 2 EMRs)

3.56 API Guideline 10 and EMI Guideline 10 set out the information and documentation which is required in relation to the applicant's process to file, monitor, track and restrict access to sensitive payment data. See also **Chapter 18 – Operational and Security Risk Management**.

Business continuity arrangements (paragraph 8 of Schedule 1 PSRs 2017 and paragraph 5C Schedule 1 EMRs)

3.57 API Guideline 11 and EMI Guideline 11 sets out the information and documentation which is required in relation to business continuity arrangements.

3.58 Statistical data on performance, transactions and fraud — paragraph 9, Schedule 2 of the PSRs 2017 and paragraph 5D, Schedule 1 of the EMRs — API Guideline 12 and EMI Guideline 12 set out the information and documentation required in relation to collection of statistical data on performance, transactions and fraud. This should demonstrate how the applicant will ensure it can meet its obligations to report to the FCA, see **Chapter 13 – Reporting**.

Security policy (paragraph 10 Schedule 1 PSRs 2017 and paragraph 5E Schedule 1 EMRs)

3.59 The security policy must include a detailed risk assessment of the services to be provided, including risks of fraud and illegal use of sensitive and personal information and the mitigation measures to protect users from the risks identified. It must also describe a high level of technical security and data protection is achieved, including IT systems used by the applicant and anyone it outsources to. Applicants should also demonstrate how they will comply with their obligation under regulation 98(1) of the PSRs 2017 (management of operational and security risk).

3.60 API Guideline 13 and EMI Guideline 13 set out the information and documentation which is required in relation to the applicant's security policy. More information on security can be found in **Chapter 18 – Operational and Security Risk Management**.

Money laundering and other financial crime controls (Paragraph 11 Schedule 2 PSRs 2017 and paragraph 6 Schedule 1 EMRs)

3.61 Applicants must provide a description of the internal control mechanisms that they will establish to comply with the Money Laundering, Terrorist Financing and Transfer of Funds (Information to the payer) Regulations 2017 and the EU Funds Transfer Regulation (EU 2015/847).

3.62 All PIs and EMIs must comply with legal requirements to deter and detect financial crime, which includes money laundering and terrorist financing. We give more detail on these requirements in **Chapter 19 – Financial Crime**. API Guideline 14 and EMI Guideline 14 set out the information and documentation required for money laundering

and other financial crime controls. We expect applicants to explain how they propose to meet their obligations under the relevant legislation.

3.63 As part of this, we expect firms to demonstrate that they establish and maintain appropriate and risk-sensitive policies and procedures to counter the risk that they may be used to further financial crime. These policies and procedures should be proportionate to the nature, scale and complexity of the firm's activities and enable it to identify, manage, monitor and report any financial crime risks to which it may be exposed. Firms should ensure they establish a clear organisational structure where responsibility for establishing and maintaining effective policies and procedures to prevent financial crime is clearly allocated (see also Governance arrangements, risk management and internal controls).

3.64 As part of the information provided by applicants, and in accordance with the Money Laundering, Terrorist Financing and Transfer of Funds (Information to the payer) Regulations 2017, we expect details on the risk-sensitive anti-money laundering policies, procedures and internal controls related to:

- customer due diligence checks
- the ongoing monitoring of business relationships
- the reporting of suspicions, both within the firm and to the National Crime Agency
- assessment of money laundering risks and the application of enhanced measures in higher risk situations
- record keeping
- monitoring compliance with procedures
- internal communication of policies and procedures
- staff awareness and training on money laundering matters

3.65 This should include the systems and controls in place to ensure that the applicant's branches and agents comply with applicable anti-money laundering and combating terrorist financing requirements in the relevant jurisdiction where the branch or agent is based.

3.66 Applicants must also provide us with the name of the person nominated to receive disclosures under Part 7 of the Proceeds of Crime Act 2002 and referred to in regulation 21(3) of the Money Laundering, Terrorist Financing and Transfer of Funds (Information to the payer) Regulations 2017 (the Money Laundering Reporting Officer). Where different, applicants must also provide us with the name of the individual appointed under regulation 21(7) of those Regulations.

Structural organisation (paragraph 12 Schedule 2 PSRs 2017, paragraph 7 Schedule 1 EMRs)

3.67 We will require a description of the applicant's structural organisation, which is the plan for how the work of the business will be organised. API Guideline 5 and EMI Guideline 5 set out the information and documentation which must be provided in relation to the structural organisation.

3.68 The information must include a description of the applicant's outsourcing arrangements (if any). The PSRs 2017 (regulation 25) and EMRs (regulation 26) make specific provisions in relation to the outsourcing to third parties of 'important' operational functions by authorised PIs and authorised EMIs including the provision to it of an information technology system. These provisions are:

- the outsourcing is not undertaken in such a way as to impair
  - the quality of internal control
  - our ability to monitor and retrace the authorised PI's or authorised EMIs compliance with the PSRs 2017 and /or the EMRs
- the outsourcing does not result in any delegation by the senior management of responsibility for complying with the PSRs 2017 and/ or the EMRs
- the relationship and obligations of the authorised PI towards its payment service users under the PSRs 2017, or the authorised EMI towards its e-money holders under the PSRs 2017 or EMRs, is not substantially altered
- compliance with the conditions which the PI or EMI must observe in order to be authorised and remain so is not adversely affected
- none of the conditions of the PI's or EMI's authorisation requires removal or variation

3.69 We will take these factors into consideration when assessing an authorisation application where the business intends to outsource important operational functions. See 'Outsourcing arrangements' in Part 2 of **Chapter 4 – Change in circumstances of authorisation or registration** for guidance on what constitutes an 'operational function'.

3.70 Regulation 25(3) PSRs 2017 and regulation 26 EMRs indicate what is considered an 'important operational function'. It is a function which, if it failed or was defective, would materially impair an authorised PI's or authorised EMI's ability to comply with the PSRs 2017 and/or EMRs and any requirements of authorisation, its financial performance, or soundness or continuity of its payment services and/or electronic money issuance. In practice, which of an authorised PI's or authorised EMI's operational functions are important will vary from business to business, according to the nature and scale of the business.

Money laundering registration (regulation 6(8) PSRs 2017 and regulation 6(7) EMRs)

3.71 Applicants that are required to be registered with HM Revenue and Customs (HMRC) under the **Money Laundering, Terrorist Financing and Transfer of Funds (Information to the payer) Regulations 2017** will need to be registered with HMRC under the MLR before we can authorise them. This will apply to:

- money service businesses (MSBs)
- bill payment service providers
- telecommunications, digital and IT payment service providers

3.72 Firms that are already MLR-registered with HMRC should supply their registration number when applying to us. If an application to HMRC is being made at the same time

as an application for authorisation, then we will still process the application, but cannot grant authorisation until the MLR registration number has been received.

3.73 We will verify with HMRC that the registration number provided to us matches a valid MLR registration for that firm.

3.74 Where we will be responsible for money laundering supervision of the applicant, no separate registration is required. This will be the case for all EMIs and (generally speaking) all PIs (unless the application only relates to the provision of money remittance services). These firms only need to complete the 'Authorised Payment Institution' or 'Authorised E-money Institution' form, as these combine both MLR registration and PSRs 2017/EMR authorisation.

Close links (regulation 6(9) and (10) PSRs 2017 and regulation 6(8) and (9) EMRs)

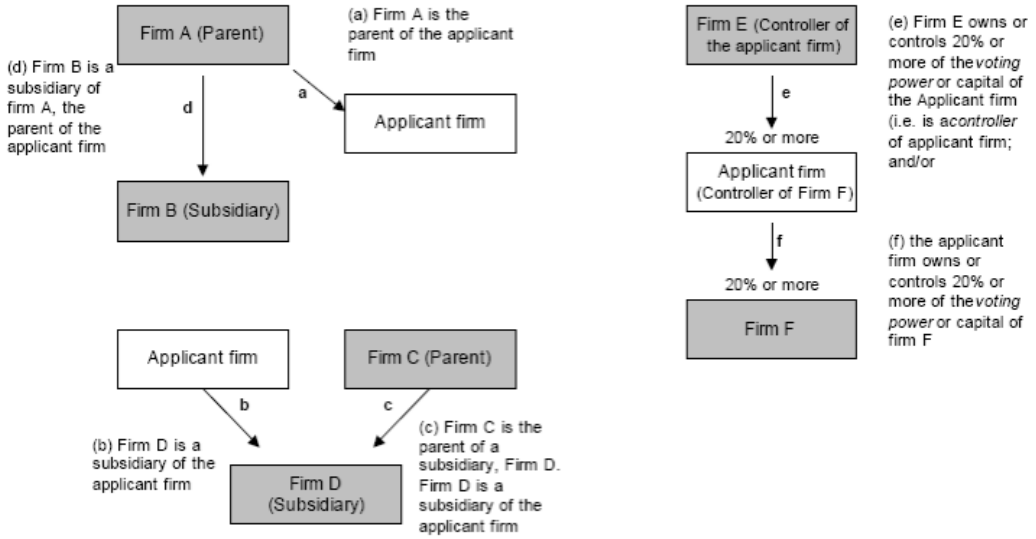
3.75 Applicants must satisfy us that any 'close links' they have are not likely to prevent the effective supervision of the firm or, where a close link is located outside of the EEA, the laws of the foreign territory would not prevent effective supervision.

3.76 A close link is defined as:

- a parent undertaking of the applicant
- a subsidiary undertaking of the applicant
- a parent undertaking of a subsidiary undertaking of the applicant
- a subsidiary undertaking of a parent undertaking of the applicant
- an owner or controller of 20% or more of the capital or voting rights in the applicant
- an entity of which the applicant owns or controls 20% or more of the capital or voting rights

3.77 The application should include details of any persons meeting the above criteria, as set out in the form. We will then assess the nature of the relationship against the conditions for authorisation.

3.78 The following diagram sets out the types of relationships between firms and individuals that meet the definition. Shaded boxes are all close links of the relevant applicant firm.



Qualifying holdings (regulation 6(7) (a), paragraph 13 Schedule 2 PSRs 2017 and regulation 6(6)(a) and paragraph 8 Schedule 1 EMRs)

3.79 A condition for authorisation under both the PSRs 2017 and EMRs is that the applicant must satisfy us that any persons having a qualifying holding in it are fit and proper persons having regard to the need to ensure the sound and prudent conduct of the affairs of the PI. This comprises two elements: firstly, the applicant will need to assess whether any persons (or entities) have a qualifying holding in the applicant and notify the FCA of their identity; and secondly, we will assess the fitness and propriety of any such persons (or entities).

3.80 A 'qualifying holding' is defined by reference to Article 4(1)(36) of Regulation (EU) 575/2013 on prudential requirements for credit institutions and investment firms. We refer to people with a qualifying holding as 'controllers'.

3.81 A controller is an individual or firm that does one of the following:

- holds 10% or more of the shares in the applicant firm (including through a parent)
- is able to exercise significant influence over the management of the applicant firm through their holding in the applicant firm or a parent
- is entitled to control or exercise control of 10% or more of the voting power in the applicant firm (including through a parent)
- is able to exercise significant influence over the management of the applicant firm through their voting power in it or a parent

3.82 Limited liability partnership (LLP) applicants should note that some (or sometimes all) individual members may be controllers of the LLP. Usually this will depend on the number of members and the terms of the membership agreement, especially regarding

voting power or significant influence. For example, in an 11-person LLP where all have equal voting power, it might appear that none of the members will be a controller (as no individual member will have 10% or more of the voting power). However, one of the members may still exercise significant influence. If the membership agreement required significant decisions to be taken unanimously by the members, a dissenting member could exercise significant influence over the firm's management despite having less than 10% of the voting power. Applicant firms should have this in mind when considering whether a member with less than 10% voting power could exercise significant influence over the firm's management.

3.83 For each qualifying holding in the applicant, an authorisation application must contain the following information:

- the size and nature of the qualifying holding
- evidence of the suitability of each controller taking into account the need to ensure the sound and prudent management of a PI

3.84 API Guideline 15 and EMI Guideline 15 set out the information and documentation which must be provided in relation to qualifying holdings. Applicants should provide this in the PI or EMI Qualifying Holdings form.

3.85 The term 'fit and proper' is used frequently in the context of individuals approved under the Financial Services and Markets Act 2000 (FSMA). We have interpreted this term, which is used in regulation 6 in relation to controllers, to mean in substance the same for PIs and EMIs as it does for individuals approved in FSMA firms. We have set out extensive guidance on what might fall within our consideration of fitness and propriety in the section of the Handbook entitled 'The Fit and Proper test for Approved Persons'. Applicants who require more information may find this guidance helpful.

3.86 In Schedule 2 to the PSRs 2017 and Schedule 1 to the EMRs, the word 'suitability' is used to describe what is required of controllers, rather than 'fitness and propriety', which is used in regulations 6. Although these terms are different, they incorporate the same essential factors, namely the:

- honesty, integrity and reputation
- competence and capability
- financial soundness

of the person with a qualifying holding having regard to the need to ensure the sound and prudent management of a PI.

3.87 Whilst it is impossible to list every fact or matter that would be relevant to the fitness and propriety of a controller, the following are examples of factors that we will consider:

- whether the person has been convicted of any criminal offence particularly of dishonesty, fraud, or financial crime

- whether the person is currently being investigated for any criminal offence. This would include where an individual has been arrested or charged

- whether the person has been the subject of any adverse finding or any settlement in civil proceedings, particularly in connection with investment or other financial business, misconduct, fraud or the formation or management of a firm, particularly a PI or an EMI. This would include any findings by us, by other regulatory authorities (including a previous regulator), clearing houses and exchanges, professional bodies, or government bodies or agencies (such as HMRC, the Serious Organised Crime Agency, the Serious Fraud Office etc.) that the individual has breached or contravened any financial services legislation. The regulatory history of the firm or individual is therefore likely to be relevant

- whether the person has been the subject of, or interviewed in the course of, any existing investigation or disciplinary proceedings, by us, by other regulatory authorities (including a previous regulator), clearing houses and exchanges, professional bodies, or government bodies or agencies (such as HMRC, the Serious Organised Crime Agency, the Serious Fraud Office etc.)

- whether the person has been refused membership, registration or authorisation of a professional organisation or has had that registration, authorisation, membership or licence revoked, withdrawn or terminated, or has been expelled by a regulatory or government body

- whether the person has been a director, partner, or concerned in the management, of a business that has gone into insolvency, liquidation or administration while the person has been connected with that organisation or within one year of that connection

- whether, in the past, the person has been candid and truthful in all his dealings with any regulatory body and whether the person demonstrates a readiness and willingness to comply with the requirements and standards of the regulatory system and with other legal, regulatory and professional requirements and standards

3.88 Importantly, we will also consider the fitness and propriety of any person linked to the controller (i.e. any person who has, or who appears to have, a relevant family or business relationship with the controller), and whether this adversely affects the suitability of the controller.

3.89 The forms are available via Connect. We attach considerable importance to the completeness and accuracy of the 'Qualifying Holding' form. If the applicant is in any doubt as to whether or not any information is relevant, it should be included.

Directors and persons responsible for payment services (regulation 6(7) (b), and paragraph 14, Schedule 2 PSRs 2017, regulation 6(6)(b) and paragraph 9, Schedule 1 EMRs)

3.90 The applicant must satisfy us that its directors and any other persons who are or will be responsible for the management of the PI or EMI and its payment services activities

and e-money issuance, are of good repute and have the appropriate knowledge and experience to perform payment services and issue e-money.

3.91 This incorporates two elements: firstly, identification by the applicant of those with responsibility for the payment service or e-money activities of the PI or EMI. All these individuals need to be included in the application (they are referred to as a 'PSD Individual' or an 'EMD Individual' as appropriate). Secondly, the applicant, together with the PSD or EMD Individual, must provide full and complete information to us about all PSD or EMD Individuals in order to satisfy us as to the reputation, knowledge and experience of these individuals. This must be done by completing the PSD Individual form or EMD Individual form for each individual. API Guideline 16 and EMI Guideline 16 sets out the information and documentation required in relation to the identity and suitability of directors and persons responsible for the management of the PI.

3.92 In the case of a PI that only provides payment services, or an EMI that only issues e-money and provides payment services, the applicant is likely to be required to complete the relevant PSD/EMD Individual forms for each and every manager of the PI/EMI, but only to the extent that their role is directly relevant to payment services or e-money issuance. For example, we would not expect a procurement manager whose responsibility is limited to sourcing and purchasing goods and services for the applicant to seek approval. Similarly, in the case of PIs and EMIs that carry on business activities other than solely payment services and/or issuance of e-money, the applicant is likely to be required to complete the relevant PSD/EMD Individual forms only for those managers with responsibility for running the firm's payment services activities and e-money issuance activities.

Assessing reputation – fitness and propriety

3.93 We will assess the fitness and propriety of an individual on the information provided in the application form and other information available to us from our own and external sources. We may ask for more information if required. We require the disclosure of convictions and cautions. Additionally, we also require the disclosure of all spent and unspent criminal convictions and cautions (other than those criminal convictions and cautions that are protected).[3] **We attach considerable importance to the completeness and accuracy of the PSD Individual form or EMD Individual form. If the applicant is in any doubt as to whether or not any information is relevant, it should be included.**

3.94 We consider the term 'of good repute' to include the essential factors relating to fitness and propriety set out above in relation to controllers. This means that we will consider the same essential factors, set out in paragraph 3.82 above in respect of all directors and all persons who are or who will be responsible for the management of the PI/EMI or its payment services and/or e-money issuance activities.

[3] The relevant legislation: the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975, the Rehabilitation of Offenders (Exceptions) Order (Northern Ireland) 1979 and the Rehabilitation of Offenders Act 1974 (Exclusions and Exceptions)(Scotland) Order 2013.

3.95 During the application process, we may discuss the assessment of the candidate's fitness and propriety informally with the firm and may retain any notes of those discussions.

3.96 The factors that we will have regard to when making the fit and proper assessment are:

- honesty, integrity and reputation
- competence and capability
- financial soundness

3.97 Examples of the matters we will consider for each factor are set out below. However, it is not possible to list all the matters that would be relevant to a particular application or individual.

Honesty, integrity and reputation

3.98 In determining the honesty, integrity and reputation of an individual, the matters that we will have regard to include, but are not limited to:

- relevant convictions or involvement in relevant criminal proceedings or ongoing investigations
- relevant civil or administrative cases
- relevant disciplinary action (including disqualification as company director or bankruptcy)
- whether the individual has been a director or senior manager in an entity that has been put into liquidation, wound up or is or has been the subject of an investigation by an inspector under company or any other legislation
- information (including relevant shareholdings) relevant for assessing potential conflicts of interest with another entity

3.99 We will consider matters that may have arisen in the UK or elsewhere.

3.100 The 'relevant' matters we refer to above will include offences under legislation relating to companies, banking or other financial services, serious tax offences or other dishonesty, insolvency, insurance, money laundering, market abuse, misconduct or fraud.

3.101 The applicant firm should tell us of all relevant matters, but we will consider the circumstances in relation to the requirements and standards of the PSRs 2017 or EMRs. For example, a conviction for a criminal offence will not automatically mean an application is rejected. We treat each individual's application on a case-by-case basis, taking into account the seriousness of, and the circumstances surrounding, the offence, the explanation offered by the convicted individual, the relevance of the offence to the proposed role, the passage of time since the offence was committed and evidence of the individual's rehabilitation.

3.102 If a firm is not sure whether something may have an impact on an individual's fitness and propriety, the information should be disclosed. The non-disclosure of material facts is taken very seriously by us as it is seen as evidence of current dishonesty. If in doubt, disclose.

Competence, capability and experience

3.103 In determining an individual's competence, capability and experience, we will have regard to whether the individual has the:

- knowledge
- experience
- training

to be able to perform the activity of providing payment services.

Financial soundness

3.104 In determining good repute, we will take into account an individual's financial soundness and we will consider any factors including, but not limited to:

- whether the individual has been the subject of any judgment debt or award in the UK or elsewhere, that remains outstanding or was not satisfied within a reasonable period
- whether the individual has made any arrangements with their creditors, filed for bankruptcy, had a bankruptcy petition served on them, been an adjudged bankrupt, been the subject of a bankruptcy restrictions order (including an interim bankruptcy restriction order), offered a bankruptcy restrictions undertaking, had assets sequestrated, or been involved in proceedings relating to any of these

3.105 The fact that an individual may be of limited financial means will not, in itself, affect their suitability to perform payment services activities.

Auditors and audit arrangements (paragraphs 15 and 18 Schedule 2 PSRs 2017, paragraph 10 and 13 Schedule 1 EMRs)

3.106 API Guideline 17 and EMI Guideline 17 sets out the information which must be provided by an applicant in relation to its statutory auditor or audit firm. Applicants are required to provide a description of the audit and organisational arrangements that have been set up in relation to the safeguarding measures, governance arrangements, risk management procedures, internal control mechanisms, security incidents and security-related customer complaints and organisational structure described in the application. These should show that the applicant is taking all reasonable steps to protect the interests of its customers and to ensure the continuity and reliability of performance of payment services and issuance of e-money. See section 3.34 above.

3.107 Depending on the nature, scale and complexity of its business, to comply with the requirement of the PSRs 2017 and EMRs for sound accounting procedures and adequate internal control mechanisms, it may be appropriate for a firm to maintain an internal audit function which is separate and independent from the other functions and activities of the firm. We would expect the internal audit function to have the following responsibilities:

- establish, implement and maintain an audit plan to examine and evaluate the adequacy and effectiveness of the firm's systems, internal control mechanisms and arrangements

- issue recommendations based on the result of work carried out
- verify compliance with those recommendations
- report in relation to internal audit matters to senior personnel and/or separate supervisory function (for example, a supervisory board in a two-tier board structure or non-executive committee in a one-tier structure)

Location of offices and where business is carried out (regulation 6(4) and (5), paragraph 17, Schedule 2 PSRs 2017, regulation 6(4) and (5) paragraph 12, Schedule 1 EMRs

3.108 An applicant to be an authorised PI must be a body corporate (for example, a limited company or limited liability partnership) constituted under the law of the UK and whose head office and, where relevant, its registered office is in the UK.

3.109 An applicant to be an authorised EMI must be either:

- a body corporate constituted under the law of the UK and whose head office and, where relevant, its registered office is in the UK
- a body corporate which has a branch that is located in the UK and whose head office is situated in a territory that is outside the EEA

3.110 The PSRs 2017 and the EMRs do not define what is meant by a firm's 'head office'. This is not necessarily the firm's place of incorporation or the place where its business is wholly or mainly carried on. Although we will judge each application on a case-by-case basis, the key issue in identifying the head office of a firm is the location of its central management and control, that is, the location of:

- the directors and other senior management, who make decisions relating to the firm's central direction, and the material management decisions of the firm on a day-to-day basis
- the central administrative functions of the firm (for example, central compliance, internal audit)

3.111 For the purpose of regulation 6(4) a ‘virtual office’ in the UK does not satisfy this condition.

3.112 In order to obtain authorisation, for a PI applicant, it is a requirement that it carries on, or will carry on, at least part of its payment service business in the UK and, for an EMI applicant, that it carries on, or will carry on, at least part of its electronic money and payment service business in the UK.

Part II: Becoming a small PI or a small EMI

This Part of Chapter 3 will be consulted on in due course by the FCA.

Part III: Becoming a RAISP

3.113 This section applies to a business that wishes to become a RAISP. The information requirements relevant to such applications can be found in regulation 17 of the PSRs 2017 and the conditions of registration are set out in regulation 18.

3.114 RAISPs may not provide any payment services other than account information services (AIS).

3.115 The application fee for RAISPs is set out in **Chapter 15 - Fees**.

3.116 The application must be signed by the person(s) responsible for making the application on behalf of the applicant firm. The appropriate persons(s) depends on the applicant firm's type, as follows:

Type of applicant	**Appropriate signatory**
Sole trader	The sole trader
Partnership	Two partners
Unincorporated association (not a limited partnership)	All members of the unincorporated association or one person authorised to sign on behalf of them all (supported by a resolution of the committee of management or equivalent)
Company with one director	The director
Company with more than one director	Two directors
Limited liability partnership	Two members
Limited partnership	The general partner or partners

Information to be provided and conditions of registration

3.117 We may refuse to register an applicant as a RAISP if the conditions in regulation 18 are not met. This includes where, if registered, the grounds in regulation 10 (cancellation of authorisation) as applied by regulation 19 would be met if the applicant was registered. This means that we will take account of those grounds — such as threats to the stability

of, or trust in, a payment system or the protection of the interests of consumers in considering your application.

3.118 This section needs to be read alongside section 4.2 ("Guidelines on information required from applicants for registration for the provision of only service 8 of Annex I PSD2 (account information services)) of the EBA Guidelines (the RAISP Guidelines). Together, these documents explain the information that you must supply with the application and the conditions that must be satisfied.

Programme of operations (paragraph 1, Schedule 2 PSRs 2017)

3.119 The information and documentation which needs to be provided in the programme of operations for RAISP applications is set out in RAISP Guideline 3.

3.120 The programme of operations to be provided by the applicant must describe the AIS to be provided and explain how this fits the definition of AIS in the PSRs 2017. As this service cannot involve coming into possession of funds, a declaration to this effect is required. In our view being in possession of funds includes an entitlement to funds in a bank account in your name, funds in an account in your name at another PI and funds held on trust for you.

Business plan (paragraph 2, Schedule 2 PSR s2017)

3.121 The information and documentation which needs to be provided in the business plan for RAISP applications is set out in RAISP Guideline 4. These are similar to those for an authorised PI (see Part I).

Governance arrangements, internal controls and risk management (paragraph 5 of Schedule 2 PSRs 2017)

3.122 The governance arrangements, internal controls and risk management requirements for applications as RAISPs are outlined in RAISP Guideline 6. Governance arrangements are the procedures used in the decision-making and control of the business that provide its structure, direction and accountability.

3.123 The description of the risk management procedures provided in the application should show how the business will effectively identify, manage, monitor and report any risks to which the applicant might be exposed.

3.124 Such risks may include, where appropriate:

- operational risk (loss from inadequate or failed internal processes, people or systems)
- counterparty risk (that the other party to a transaction does not fulfil its obligations)
- liquidity risk (inadequate cash flow to meet financial obligations)
- market risk (risk resulting from movement in market prices)
- financial crime risk (the risk that the PI or its services might be used for a purpose connected with financial crime)
- foreign exchange risk (fluctuations in exchange rates)

3.125 Depending on the nature and scale of the business it may be appropriate for the RAISP to operate an independent risk management function. Where this is not appropriate, the RAISP should be able to demonstrate that the risk management policies and procedures it has adopted are effective. See **Chapter 18 – Security and operational risk**.

3.126 Internal controls are the systems, procedures and policies used to safeguard the business from fraud and error, and to ensure accurate financial information. They should include sound administrative and accounting procedures that will enable the applicant to deliver to us, in a timely manner, financial reports that reflect a true and fair view of its financial position and that will enable the applicant to comply with the requirements of the PSRs 2017 in relation to its customers.

Security incidents and security-related customer complaints (paragraph 6 Schedule 2 PSRs 2017)

3.127 The information and documentation which needs to be provided in for security incidents and security-related customer complaints requirements for applications as RAISPs are set out in RAISP Guideline 7. The information required includes details of how the applicant will comply with its obligation to report major operational or security incidents under regulation 99 PSRs 2017.

Sensitive payment data (paragraph 7 Schedule 6 PSRs 2017)

3.128 The information and documentation relating to sensitive payment data applicants are required to provide are set out in RAISP Guideline 8. Applicants must provide a description of the process in place to file, monitor, track, and restrict access to sensitive payment data including, for example, a list of the data classified as sensitive payment data in the context of the RAISP's business model and the procedures in place to authorise access to the sensitive payment data. See also **Chapter 18 - Operational and security risk management.**

Business continuity arrangements (paragraph 8 Schedule 2 PSRs 2017)

3.129 The information and documentation which needs to be provided with respect to business continuity requirements for applications as RAISPs are set out in RAISP Guideline 9. Applicants must provide a description of their business continuity arrangements including, for example, a business impact analysis and an explanation of how the applicant will deal with significant continuity events and disruptions.

Security policy document (paragraph 10 of Schedule 2 PSRs 2017)

3.130 The security policy must include a detailed risk assessment in relation to the services to be provided, including risks of fraud and illegal use of sensitive and personal information and the mitigation measures to protect users from the risks identified. It must also describe how such measures ensure a high level of technical security and data protection, including in relation to IT systems used by the applicant and any one it outsources to. Applicants should also demonstrate how they will comply with their obligation under regulation 98(1) (management of operational and security risk).

3.131 The information and documentation to be provided in relation to the security policy document is outlined in RAISP Guideline 10. More information on security can be found in **Chapter 18 - Operational and Security Risk Management**.

Structural organisation (Paragraph 12 of Schedule 2 PSRs 2017)

3.132 We will require a description of the applicant's structural organisation, which is the plan for how the work of the business will be organised. The information and documentation to be provided on the structural organisation of applicants as RAISPs are detailed in RAISP Guideline 5. While details of outsourcing arrangements must be provided, RAISPs should note that regulation 25 PSRs 2017 does not apply to them so, for example, they will not be subject to requirements such as notifying the FCA of their intention to enter into an outsourcing contract relating to the provision of payment services.

Directors and persons responsible for payment services (Paragraph 14 of Schedule 2 PSRs 2017)

3.133 The information requirements relating to the directors and persons responsible for the payment services of RAISPs are set out in RAISP Guideline 11. These information requirements include personal details, information relating to financial and non-financial interests and information on any other professional activities carried out.

Auditors and audit arrangements (Paragraph 18 of Schedule 2 PSRs 2017)

3.134 RAISP Guideline 17 sets out the information which must be provided by an applicant in relation to its statutory auditor or audit firm.

3.135 Paragraph 18 of Schedule 2 PSRs 2017 requires the applicant to provide a description of the audit and organisational arrangements that have been set up in relation to the governance arrangements, risk management procedures, internal control mechanisms, security incident and security related customer complaints and organisational structure described in the application.

Professional Indemnity insurance (PII) (paragraph 19, Schedule 2 PSRs 2017)

3.136 The applicant must satisfy the FCA that it holds appropriate professional indemnity insurance or a comparable guarantee. RAISP Guideline 12 sets out the information and documentation which is required in relation to this insurance or guarantee.

Part IV: Decision-making process

3.137 Having assessed the application and all the information provided, we will make a decision to either approve or reject the application. This decision will be notified to the applicant, along with instructions for the appeal process, if relevant.

Timing (regulation 9(1) and (2) PSRs 2017, regulation 9(1) and (2) EMRs)

3.138 We have to make a decision on a complete application within three months of receiving it. An application is only complete when we have received all the information and

evidence needed for us to make a decision. We will let the applicant know if we need more information.

3.139 In the case of an incomplete application, we must make a decision within 12 months of receipt. However, if that date is reached and discussions with the firm have not resulted in us receiving all the information we need, it is likely that an incomplete application will result in a refusal. This is because it is unlikely we will have been able to satisfy ourselves that the applicant has met the authorisation/registration requirements.

Withdrawal by the applicant (regulation 9(3) PSRs 2017, regulation 9(3) EMRs)

3.140 An application may be withdrawn by giving us written notice at any time before we make a decision. The application fee is non-refundable.

Approval (regulation 9(5) and (6) PSRs 2017, regulation 9(4) and (5) EMRs)

3.141 If we decide to grant an application we will give the applicant notice of that decision. This notice will specify the activities for which approval has been granted, requirements (if applicable) and the date from which it takes effect.

3.142 The PSRs 2017 allow us to vary the types of payment services that a PI is ultimately approved to carry out from those requested in the application. Both the EMRs and PSRs 2017 allow us to apply requirements that we consider appropriate to the PI or EMI as a condition of authorisation or registration (regulation 7 PSRs 2017 and regulation 7 EMRs). This may include requiring the business to take a specified action or refrain from taking a specified action (for example, not to deal with a particular category of customer). The requirement may be imposed by reference to an applicant's relationship with its group or other members of its group. We may also specify the time that a requirement expires.

3.143 Where an applicant carries on business activities other than the issuance of e-money and/or provision of payment services (as the case may be) and we feel that the carrying on of this business will, or is likely to, impair our ability to supervise the firm or its financial soundness, we can require the applicant firm to form a separate legal entity to issue the e-money and/or perform payment services.

3.144 We will update the online register as soon as possible after granting the authorisation or registration. The register will show the contact details of the firm, the payment services it is permitted to undertake, and the names of any agents. If the firm is authorised and has taken up passporting rights to perform payment services in another EEA State, then these will also be shown.

Refusal (regulation 9(7) to (9) PSRs 2017, regulation 9(6) to (8) EMRs)

3.145 We can refuse an application when the information and evidence provided does not satisfy the requirements of the PSRs 2017 or EMRs. When this happens we are required to give the applicant a warning notice setting out the reason for refusing the application and allowing 28 days to make a representation on the decision.

3.146 Applicants can make oral or written representations. If oral representations are required, we should be notified within 2 weeks of the warning notice, so that arrangements can be made for a meeting within the 28 day deadline.

3.147 If no representations are made, or following them we still decide to refuse the application, we will give the applicant a decision notice. If a firm wishes to contest the decision, they may refer the matter to the Upper Tribunal (Financial Services), an independent judicial body. If no referral has been made within 28 days we will issue a final notice. If the matter is referred to the tribunal, we will take action in accordance with any directions given by it (including to authorise/register the firm) and then issue the final notice.

3.148 On issuing the final notice, we are required to publish such information about the matter to which a final notice relates as we consider appropriate. However, we may not publish information if we believe it would be unfair to the firm or prejudicial to the interests of consumers.

Part V: Transitional provisions (regulations 151 to 153 PSRs 2017, regulation 78A EMRs)

3.149 In order to continue providing payment services PIs and EMIs authorised or registered under the 2009 regulations or the EMRs must be re-authorised or re-registered. They must also pay a fee, as set out in **Chapter 15 - Fees**.

PIs

3.150 An authorised PI must provide to the FCA the information specified in the PSRs 2017 and the API Guidelines that it has not previously provided (whether as part of its original authorisation or otherwise). This information must be provided (or the firm must notify the FCA that it has already been provided) by 12 April 2018 in order to continue providing payment services on or after 13 July 2018.

3.151 The FCA will treat this as an application for authorisation under the PSRs 2017, and assess in accordance with the guidance set out in this chapter.

3.152 A small PI must apply for registration under the PSRs 2017 by 13 October 2018 if it wants to continue providing payment services as a small PI on or after 13 January 2019. The information that must be provided in support of this application is the information that is required in an application for registration under the PSRs 2017 where this has not already been provided (or where there has been a material change since they provided it).

3.153 The application for registration under these provisions will be assessed in the normal way.

3.154 An authorised PI that provides payment services on or after 13 July 2018 and a small PI that provides payment services on or after 13 January 2019 without complying with the above are at risk of committing a criminal offence under regulation 138 (prohibition on provision of payment services by persons other than payment service providers).

EMIs

3.155 An authorised EMI must provide to the FCA the information specified in the EMRs (as amended) and the EMI Guidelines that it has not previously provided (whether as part of its original authorisation or otherwise). This information must be provided (or the firm must notify the FCA that it has already been provided) by 12 April 2018 in order to continue issuing e-money or providing payment services on or after 13 July 2018.

3.156 A small EMI that intends to provide services on or after 13 July 2018 as a small EMI must notify the FCA whether it continues to meet the requirements for registration, and provide any information relevant to that question, by 12 April 2018.

3.157 On receipt of this information the FCA will consider whether the EMI's authorisation or registration should be continued after 13 July 2018. If the FCA does not decide to continue the EMIs authorisation or registration it is treated as cancelled on 13 July 2018.

3.158 Firms which fall into these categories needs to complete an 'Application to Retain Authorisation/Registration' form and submit it to us along with the required information and the appropriate application fee within the specified timeframes outlined above.

3.159 Application forms are available on the payment services section of our website.

3.160 Under regulation 78A(2)(b) EMRs, EMIs authorised before 13 January 2018 are subject to an automatic requirement on their authorisation, preventing them from providing AIS or PIS. If authorised EMIs wish to provide these services, they will need to apply to us to have this requirement removed. Small EMIs cannot provide AIS or PIS.

Payments through network operators

3.161 Where a PI provided payment services of the type described in paragraph 1(g) of Schedule 1 to the PSRs 2009 prior to 13 January 2018, it is not required to seek re-authorisation or re-registration in order to provide those services. It must, however, provide evidence to the FCA before 13 January 2020 that it complies with relevant own funds requirements.

In flight applications

3.162 Where a firm has applied for authorisation or registration under the PSRs 2009 but whose application has not been determined before 13 January 2018, they are automatically treated as applications under the PSRs 2017. They will be required to provide the additional information (if they have not already done so) before we can determine their application.

4. Changes in circumstances of authorisation or registration

4.1 This chapter describes the notifications that authorised and small PIs and EMIs need to make to us as part of their ongoing authorisation or registration. It is divided into three parts.

- Part I – Notifications applicable to all EMIs and PIs.
- Part II – Notifications applicable only to authorised PIs and EMIs.
- Part III – Notifications applicable only to small PIs and EMIs.

4.2 Credit institutions, credit unions and municipal banks with Part 4A permission to issue e-money may apply to vary their permission under the FSMA process. Information on that process can be found in chapter 6 of the supervision manual of the Handbook.

Introduction

4.3 PIs and EMIs need to provide us with two types of regulatory information – we categorise these as 'reporting' and 'notifications'.

4.4 Reporting information is the information we need on a regular and periodic basis to comply with our supervisory and EU reporting obligations. Reporting requirements are discussed in **Chapter 13 – Reporting and notifications**.

4.5 The subject of this chapter is the notifications that PIs and EMIs need to send us when there is a change in the information they have already provided. The PSRs 2017 also set out other reporting and notification requirements that are not discussed in this chapter. This includes obligations on all firms including account servicing payment service providers and firms operating under exclusions from the scope of the PSRs. Firms should review **Chapter 13 – Reporting and notifications**, which provides further information.

4.6 There are other notification requirements relating to significant changes that are not covered in this chapter. Where a PI or EMI (whether small or authorised) is using an agent, they must notify us where there are significant changes that are relevant to the fitness of directors and managers of the agent or to the risk of money laundering or terrorist financing through the agent. An authorised PI or authorised EMI must also notify us where there are significant changes relevant to their provision of payment services or issuing, distributing or redeeming e-money in the exercise of passport rights. These are covered in **Chapter 5 – Appointment of agents** and **Chapter 6 – Passporting**.

Types of notifications and timing

4.7 The PSRs 2017 and the EMRs contain requirements in relation to notifications of changes in specific circumstances, as well as a general requirement in regulation 37 of the PSRs 2017 and regulation 37 of the EMRs.

4.8 The general requirement is that where it becomes apparent to a PI or EMI that there is, or is likely to be, a significant change in circumstances, which is relevant to its fulfilment of the conditions for authorisation or registration, it must provide us with details of the change without undue delay. We generally consider 'without undue delay' to mean within 28 days of the change occurring at the latest.

4.9 Regulation 37 of the PSRs 2017 also requires that in the case of a substantial change which has not yet taken place, the PI must provide details of the change in good time before the change takes place. A 'substantial change' is, in our view, one that could impact on either the firm's ability to meet the conditions for remaining authorised or registered, or the way we would supervise the firm. We will need to assess substantial changes against the initial conditions for authorisation or registration. To give us time to do this, we consider that a period of 28 days before the change takes place would generally be 'in good time'. However, in some circumstances we would expect to be notified further in advance. The notification period will depend on the circumstances of the change and firms should make efforts to notify us as soon as possible. The Customer Contact Centre can provide further guidance.

How to notify us

4.10 Notifications must be made using the relevant form available on the payment services or e-money institution section of our website, as relevant, or, where a form is not provided, by written confirmation to our Customer Contact Centre.

Different notifications for authorised and small PIs and EMIs

4.11 Not all notification requirements apply to both authorised and small PI and authorised and small EMIs.

4.12 This is mostly due to authorised PIs/EMIs having to meet more initial conditions that could change over the life of the business. Although most of the notification requirements that apply to a small PI/small EMI also apply to an authorised PI/authorised EMI, some do not.

Part I: Notifications applicable to authorised and small PIs and EMIs

4.13 Changes in the information set out below will require a notification to us.

Name, contact details and standing data (including firm name and contact details)

4.14 PIs and EMIs should give us reasonable advance notice of changes to their name and contact details, which includes:

- legal name (registered name, in the case of an authorised PI/EMI);
- trading name (if applicable);
- principal place of business;
- registered offices or branch;[4]
- primary compliance contact;
- accounting reference date; and
- website and email address.

4.15 Pursuant to regulations 37(2) and 37(3) of the PSRs and EMRs, respectively, notifications must be made using the relevant form available on the payment services or e-money institution section of our website, as relevant, or, where a form is not provided, by written confirmation to our Customer Contact Centre.

Significant changes to the programme of operations

4.16 We would expect to be notified by the PI or EMI of any significant changes to the business. This may include proposed restructuring, reorganisation or business expansion that could have a significant impact on the firm's risk profile or resources. For EMIs this could include changes to the EMI's distributors. As noted above, PIs and EMIs must notify us of certain significant changes that are covered in **Chapter 5 – Appointment of agents** and **Chapter 6 – Passporting**.

4.17 We would also expect to be advised of any proposed action that is likely to result in an EMI or PI being unable to meet its capital requirements, including but not limited to:

- any action that would result in a material change in the EMI's or PI's financial resources or financial resources requirement;
- a material change resulting from the payment of a special or unusual dividend or the repayment of share capital or a subordinated loan;
- significant trading or non-trading losses (whether recognised or unrecognised); and failures in governance arrangements and internal control mechanisms.

4.18 An EMI or PI should notify the Customer Contact Centre of any significant failure in its systems or controls, including those reported to the EMI or PI by its auditor (if applicable). Reporting requirements covered by regulation 99 of the PSRs 2017 (and

[4] This means any place of business other than the PI or EMI's head office, which forms a legally dependent part of such a payment service provider and which carries out directly all or some of the services inherent in the business of such a payment service provider. See Regulation 2 of the PSRs 2017.

European Banking Authority Guidelines on major incidents reporting under the Payment Services Directive 2) also apply.

Changes in methods of safeguarding

4.19 Given the crucial importance of safeguarding, it is necessary that we are informed by PIs and EMIs in advance of any material change, such as a change in the method of safeguarding, a change in the credit institution where safeguarded funds are deposited, or a change in the insurance undertaking or credit institution that insured or guaranteed the safeguarded funds.

Changes in methods of safeguarding

4.20 When an EMI or PI becomes aware that a change to the money laundering reporting officer has occurred or will occur, it should notify us without undue delay.

Changes in control

4.21 The following paragraphs are relevant to authorised EMIs, authorised PIs and small EMIs and to persons deciding to acquire, increase or reduce control or to cease to have control over such businesses.

4.22 In accordance with paragraph 4 of Schedule 3 to the EMRs and paragraph 4 of Schedule 6 of the PSRs 2017, the change in control provisions of FSMA (Part 12) apply (with certain modifications) to a person who decides to acquire, increase or reduce control or to cease to have control over an EMI or authorised PI[5]. Our approach to changes in control over EMIs and authorised PIs will be the same as our approach to changes in control over firms authorised under FSMA (except where stated below). Chapter 11 of the Supervision manual (in particular, SUP 11.3 and SUP 11 Annex 6G) provides guidance on the change in control provisions of FSMA.

4.23 Section 178(1) of FSMA (as modified by Schedule 3 and Schedule 6 to the EMRs and PSRs 2017, respectively) requires a person who decides to acquire or increase control over an EMI or authorised PI to notify us in writing. This notice is referred to as a 'section 178 notice'. Section 191D(1) of FSMA (as modified) provides that a person who decides to reduce or cease to have control over an EMI or authorised PI must give us written notice before making the disposition.

4.24 This means that we would expect to be notified where a person wishes to acquire, increase or reduce control, or to cease to have control over an authorised PI or an EMI and this causes them to pass a "qualifying holding" threshold (10%, 20%, 30% or 50% control, or a holding that makes it possible to exercise a significant influence over the management of the authorised PI / EMI), the individual will need to notify the FCA.

4.25 Our approval is required before any acquisition of or increase in control can take place. We have 60 working days (which can be interrupted and put on hold for up to another

[5] To date, the FCA has not exercised the power under paragraph 4(d) of Schedule 3 of the EMRs to disapply the change in control regime for EMIs carrying on business activities other than the issuance of e-money and payment services.

30 working days) to decide whether to approve, approve with conditions or object to the proposed changes.[6]

4.26 When considering a proposed acquisition or increase in control, we must consider the suitability of the person and the financial soundness of the acquisition of the qualifying holding (or control) to ensure the continued sound and prudent management of the EMI or authorised PI.[7] We must also consider the likely influence that the person will have on the EMI or authorised PI but we cannot consider the economic needs of the market (see **Chapter 3 – Authorisation and registration**, especially regarding qualifying holdings).

4.27 We may only object to an acquisition of or increase in control if there are reasonable grounds for doing so based on the criteria in section 186 of FSMA, or if the information provided by the person proposing to acquire or increase control is incomplete.

4.28 If we consider that there are reasonable grounds to object to the proposed change, we may issue a warning notice, which may be followed by a decision notice and final notice. There is a process for making representations and referring the matter to the Tribunal. Where we have given a warning notice, a decision notice or a final notice, we may also give a notice imposing one or more restrictions on shares or voting power (a restriction notice). Under the EMRs / PSRs, when issuing a restriction notice the FCA must direct that the voting power subject to the restriction notice is suspended until further notice (this differs from the FSMA regime, under which the suspension of voting rights is within our discretion).

4.29 Persons that acquire or increase control without prior approval, or in contravention of a warning, decision or final notice, may have committed a criminal offence. We may prosecute and if found guilty the person may be liable to an unlimited fine or even given a prison sentence.

4.30 The form of notice that must be given by a person who decides to acquire or increase control over an EMI or authorised PI, and the information that must be included in the notice and the documents that must accompany it, will be the same as apply to a section 178 notice in respect of an acquisition of or increase in control over an authorised person under FSMA. Notice given to us by a person who decides to acquire or increase control over an EMI and authorised PI must contain the information and be accompanied by such documents as are required by the relevant FCA controllers form. A link to this form is available on the e-money section of the website.

4.31 A notice given to us by a person who is reducing or ceasing to have control over an EMI or authorised PI should be in writing and provide details of the extent of control (if any) which the controller will have following the change in control.

---

6 See section 178 to 191 of FSMA.

7 Also see regulation 6(6)(a) of the EMRs.

Qualifying holdings

4.32 In relation to PIs and EMIs, we consider changes in qualifying holdings 'significant' in relation to changes in the circumstances of authorisation or registration. Therefore we expect to be notified by the institution of changes in qualifying holdings in good time before the change takes place. Notification should be on the appropriate 'Application for a Change in Qualifying Holding' form, which is available on the payment services section of our website.

4.33 For small PIs only, if we consider that the proposed change has an adverse impact on the small PI's fulfilment of the conditions for registration, we will advise the small PI of our concerns. If the change then goes ahead and we believe any of the relevant conditions of regulations 10 or 12 of the PSRs 2017 are met, we may take action to cancel the registration of the small PI and remove it from the register using our powers to cancel registration under regulation 10, or to impose requirements on an small PI's registration under regulation 12.

Other changes affecting controllers and close links

4.34 A condition for authorisation is that anyone with a qualifying holding in an authorised EMI or PI (a controller) must be a 'fit and proper' person. A further condition for authorisation is that, if it has close links with another person it must satisfy us that those links are not likely to prevent our effective supervision. We expect the authorised EMI or PI to notify us if there are or will be significant changes likely to affect these conditions without undue delay, under regulation 37 of the PSRs 2017. This is in addition to the annual reporting requirements (see **chapter 13 – Reporting and notifications** for further information).

Directors and persons responsible for management

Appointment and removal

4.35 Changes to the directors or persons responsible for management of either the PI/EMI or the activities of the PI/EMI are regarded as a significant change. The authorised EMI or PI should notify us of appointments before the change takes place, and removals no later than seven working days after the event.

4.36 For PIs, notification of a new appointment should be made using Connect, and should include all the information required for us to assess the individual against the requirement in regulations 6 and 13 of the PSRs 2017 to be of good repute and possess appropriate knowledge (see Part I, **Chapter 3 – Authorisation and registration**). An individual who is a member of the management staff who moves from being a non-board member to a board member will need to resubmit the relevant form on Connect.

4.37 For EMIs, notification of a new appointment should be on the EMD Individual form, which is available on the e-money section of our website, and should include all the information required for us to assess the individual against the requirements in regulation 6(6)(b) or 13(7)(a) (as appropriate) to be of good repute and possess appropriate knowledge (see **Chapter 3 – Authorisation and registration**).

4.38 PIs and EMIs must also notify us of any changes in the details of existing PSD / EMD individuals, such as name changes and matters relating to fitness and propriety. PIs should do this using the **'Notification of changes to PSD individual'** form, which is available on the payment services section of our website. EMIs should do this using the **Amend an EMD Individual** form, which is available on the e-money section of our website.

4.39 If we consider that the proposed change has an adverse impact on the PI or EMI we will advise the firm of our concerns. Where we believe the proposed change will have an adverse impact on a PI or EMI, we have the power under regulations 12 of the PSRs 2017 and regulation 11 of the EMRs to vary the PI/EMI authorisation or registration by imposing such requirements as we consider appropriate. If the change then goes ahead and we believe that any of the relevant conditions of regulation 10 of the PSRs 2017 and regulation 10 of the EMRs relating to cancellation of authorisation or registration are met, we may take action to cancel the authorisation or registration of the PI or EMI and remove it from the register, or seek to impose requirements on a PI's or EMI's authorisation or registration under regulation 12 of the PSRs 2017 and regulation 11 of the EMRs.

4.40 Information about the removal of 'directors/persons responsible' should include the reason for the departure and provide further information if the individual was dismissed for reasons potentially relating to criminal or fraudulent activities.

4.41 Notification for PIs should be on the 'Notice to remove PSD individual(s)' form which is available on the payment services section of our website. For EMIs it must be made on the Remove an EMD Individual form, which is available on the e-money section of our website. For more information on the fit and proper requirement for directors and persons responsible for management of the PI or EMI see **Chapter 3 – Authorisation and registration.**

Changes affecting the fitness and propriety of individuals

4.42 Where a PI or EMI becomes aware of information that may have an impact on the fit and proper condition applying to 'directors/persons responsible' for management of the PI/EMI and/or its payment services and/or e-money issuance activities (as applicable) the PI should notify us using the 'Notification of changes to PSD individual' form and the EMI should use the Amend an EMD Individual form, as detailed above. We will examine the information, assess it against the fitness and propriety requirements explained in **Chapter 3 – Authorisation and registration**, and notify the PI or EMI of the action that we intend to take.

Variation of payment services

4.43 When a PI or EMI intends to change the payment services or e-money issuance it is providing (either by adding or removing a service) or wants to have a new requirement imposed or an existing requirement varied or removed, it needs to apply to us for approval.

4.44 Regulations 5 and 13 of the PSRs 2017 and regulations 5 and 12 of the EMRs require that an application for variation in authorisation or registration (respectively) must:

- contain a statement of the desired variation;
- contain a statement of the e-money issuance or payment services that the applicant proposes to carry on if the authorisation/registration is varied; and
- contain or be accompanied, by such other information as we may reasonably require.

4.45 Applicants should complete and submit the 'Variation of PSD Authorisation/ Registration' or the 'Variation of EMRs Authorisation/ Registration' form, as relevant. Each is available on the payment services section or the e-money section, respectively, of our website. This sets out the information that must be provided. However, we may ask for more information if we consider it necessary to enable us to determine the application. The application fee to vary an authorisation or registration is [to be confirmed].

4.46 No work will be done on processing the application until the full fee is received. The fee is non-refundable and must be paid by cheque.

4.47 We may approve the variation in authorisation or registration (or requirements, if applicable) only if the initial conditions for authorisation/registration are being or are likely to be met (regulations 6 and 14 of the PSRs 2017 and regulations 6 and 13 of the EMRs).

Determining a variation – PIs and EMIs

4.48 The process for determining a variation is the same as for initial authorisation/registration (see Parts I and II, **Chapter 3 – Authorisation and registration**) and the time allowed for us to do this is three months. However, we expect to be able to process complete applications for variation quicker than an initial authorisation/registration, and our expected turnaround times will in most cases be quicker than this. Where firms want to increase the range of services they provide they will need to factor in the time needed for approval.

MLR registration

4.49 PIs and EMIs should notify the Customer Contact Centre immediately if there is a change in the status of their MLR registration with HMRC. See **Chapter 3 – Authorisation and registration** for more details of MLR registration requirements.

Cancellation of authorisation/registration

4.50 PIs and EMIs can request to cancel their authorisation or registration (regulation 10 and 14 of the PSRs 2017, and regulations 10 and 15 of the EMRs, respectively). PIs should use the 'Cancellation of Authorisation or Registration' form, which is available on the payment services section of our website. EMIs should use the Cancellation of Authorisation or Registration form, which is available on the e-money section of our website. We will remove the PI from the Financial Services Register, once we have established that there are no outstanding fees to either us or the FOS, that any liabilities to customers have either been paid or are covered by arrangements explained to us, and there is no other reason why the PI or EMI should remain on the Financial Services Register.

4.51 We can cancel an EMI's or PI's authorisation or registration on our own initiative when:

- the EMI has not issued e-money or the PI has not provided payment services within 12 months of becoming authorised or registered;
- the EMI or the PI ceases to engage in business activity for more than six months;
- the EMI or PI requests or consents to the cancellation
- the EMI or PI no longer meets or is unlikely to meet certain conditions of authorisation or registration or the requirement to maintain own funds;
- the EMI or PI fails to inform us of a major change in circumstances which is relevant to its meeting the conditions of authorisation or registration or the requirement to maintain own funds, as required by regulation 37;
- the EMI or the PI has obtained authorisation through false statements or any other irregular means;
- the EMI has issued e-money or provided payment services or the PI has provided payment services other than in accordance with its permissions;
- the EMI or PI constitutes a threat to the stability of, or trust in, a payment system;
- the EMI's issuance of e-money or provision of payment services or the PI's issuance of payment services is unlawful; or where the cancellation is desirable in order to protect the interests of consumers.

4.52 Where we propose to cancel an EMI or PI's authorisation or registration other than at the EMI or PI's request, the EMI or PI will be issued with a Warning Notice for which it can make representations. If the cancellation goes ahead, the EMI or PI will be issued with a Decision Notice (see **Chapter 14 - Enforcement**).

4.53 Our fee year runs from 1 April until 31 March, so if a PI or EMI applies to cancel after 31 March, full annual fees will become payable as there are no pro-rata arrangements or refunds of fees.

Change in legal status

4.54 A change in legal status (for example, limited liability partnership (LLP) to limited company) is a significant change to the authorisation/registration of the PI or EMI. Such a change is effected by cancelling the existing legal entity authorisation/registration and arranging for the authorisation/registration of the new legal entity. PIs should apply using the appropriate 'Change of Legal Status' form, which are available on the payment services section of our website. EMIs should use the Change of Legal Status form that is available on the e-money section of our website.

Part II: Notifications applicable only to authorised PIs and EMIs

4.55 This part gives examples of changes that are likely to impact the conditions for authorisation of an authorised PI or EMI. As noted in the introduction, the duty to notify changes in circumstances is general and we will expect businesses to notify us of any significant change in circumstances, including changes not set out in this chapter, which are relevant to the continued fulfilment of the conditions for authorisation.

Outsourcing arrangements

4.56 An authorised PI must inform us when it intends to enter into an outsourcing contract where it will be relying on a third party to provide an 'operational function relating to its provision of payment services' (regulation 25(1) of the PSRs 2017). The corresponding requirement for EMI relates to an EMI's intention to enter into an outsourcing contract where it will be relying on a third party to provide an 'operational function relating to the issuance, distribution or redemption of e-money or the provision of payment services (outsourcing)' (regulation 26(1)).

4.57 In our view, 'operational functions relating to provision of payment services' for PIs and 'operational functions relating to the issuance, distribution or redemption of e-money or the provision of payment services' for EMIs does not include the provision of any services that do not form part of these services (for example, legal advice, training or security) or the purchase of standardised services, including market information services.

4.58 A proposed outsourcing arrangement, relating to both PIs and EMIs, that is classified as 'important' under regulation 25(2) and (3) of the PSRs 2017 and regulation 26(2) and (3) of the EMRs, respectively, is more likely to be relevant to a PI's or EMI's compliance with the authorisation conditions than one that is not 'important'. Where an authorised PI or EMI changes its important outsourcing arrangements without entering into a new outsourcing contract, it will need to consider whether the change is relevant to the conditions for authorisation and so needs to be notified under regulation 37 of the PSRs 2017 or regulation 37 of the EMRs.

4.59 Notification of changes to outsourcing requirements should be made to the Customer Contact Centre. Depending on the nature of the arrangement, we may request further information. Changes in outsourcing functions or the persons to which the functions are outsourced must be notified without undue delay.

Auditors

4.60 Where an authorised PI or EMI has an auditor and is aware that a vacancy in the office of auditor will arise or has arisen, it should:

- notify us of the date, without delay, giving the reason for the vacancy;
- appoint an auditor to fill any vacancy in the office of auditor that has arisen;
- ensure that the replacement auditor can take up office at the time the vacancy arises or as soon as reasonably practicable after that; and

- notify us of the appointment of an auditor, giving us the name and business address of the auditor appointed and the date from which the appointment has effect.

4.61 Notifications on changes to auditors should be made to the Customer Contact Centre .

Part III: Notifications applicable only to small PIs

Change in status of a small PI

4.62 Where a small PI no longer fulfils the conditions for registration as a small PI or intends to provide services other than those that small PIs are permitted to offer under regulation 32 of the PSRs 2017, the small PI must apply for authorisation within 30 days of becoming aware of the change in circumstances if it intends to continue providing payment services in the UK (regulation 16 of the PSRs 2017). This should be done by completing an Authorised Payment Institution application form (see 3.11 onwards), and a 'Cancellation of Authorisation or Registration' form in respect of its small PI registration.

4.63 If a small PI no longer fulfils any of the other conditions for registration (See Part II - **Chapter 3 – Authorisation and registration** and regulation 14 of the PSRs 2017), it should inform us immediately.

Change in status of a small EMI (regulation 16, EMRs)

4.64 If a small EMI no longer fulfils the conditions for registration outlined in regulation 8(2)(c) or (d) (as applied by regulation 15)[8] it must, within 30 days of becoming aware of the change in circumstances, apply to become an authorised EMI if it intends to continue issuing e-money in the UK.

[8] Regulation 15 modifies the requirements set out in regulation 8 to reflect the conditions for authorisation applicable to small EMIs set out in regulation 13.

5. Appointment of agents and use of distributors

5.1 This chapter describes the application process for PIs and EMIs to register their agents with us. It also covers the appointment of distributors by EMIs. Other chapters in this document are also relevant to the appointment of agents and distributors. These include **Chapter 4 – changes in circumstances of authorisation and registration** and **Chapter 6 – Passporting**, especially paragraphs 4.6 and 6.5, 6.12 to 6.18 and 6.21 to 6.29.

Introduction

PIs and EMIs

5.2 All PIs and EMIs may provide payment services through agents, as long as they register them with us first. An agent is any person who acts on behalf of a PI or EMI in the provision of payment services (see the definition of agent in regulation 2 of the PSRs 2017).

5.3 Regulation 34 of the PSRs 2017 and regulation 33 of the EMRs set out the requirements for the use of agents. In addition, regulation 36(2) of the PSRs 2017 and regulation 36(2) of the EMRs makes PIs and EMIs responsible for anything done or omitted by an agent. PIs and EMIs are responsible to the same extent as if they had expressly permitted the act or omission. We expect PIs and EMIs to have appropriate systems and controls in place to effectively oversee their agents' activities.

5.4 An authorised PI or EMI wanting to use a passport to provide payment services into another EEA member state may use an agent to provide those services, subject to additional notification requirements (see **Chapter 6 - Passporting**). This is not relevant to small PIs or small EMIs, as they are not permitted to passport into other EEA member states.

5.5 Regulation 33 of the EMRs states that an EMI may distribute or redeem e-money through an agent or a distributor, but may not issue e-money through an agent or distributor.

5.6 Unlike agents, distributors cannot provide payment services and there is no requirement to register distributors, so it is important to understand the difference between the two. In our view, a person who simply loads or redeems e-money on behalf of an EMI would, in principle, be considered to be a distributor.

5.7 As with agents, an EMI is responsible for anything done or omitted by a distributor. An authorised EMI may engage a distributor in the exercise of its passporting rights, subject to regulation 28 of the EMRs.

RAISPs

5.8 RAISPS are not subject to the requirements relating to agents in regulation 34 or 36(2) of the PSRs 2017. A RAISP wanting to use an agent to provide payment services in another member state must provide details of their EEA agents as part of their passporting notification, and these agents will be added to the Financial Services Register.

Applying to register an agent

5.9 PIs who want to register an agent must do so through the FCA Connect system. Application templates for the registration of agents can be found on the payment services section of our website. The same form is used for agents of authorised and small PIs.

5.10 EMIs who want to register an agent must submit the *Add EMD agent* application form, which can be found on the e-money section of our website. The same form is used for agents of authorised and small EMIs.

5.11 This is the information required for the registration of an agent in accordance with regulation 34 of the PSRs 2017 or regulation 34 of the EMRs:

- the name and address of the agent
- where relevant, a description of the internal control mechanisms that will be used by the agent to comply with the provisions of the money laundering directive (or, in the United Kingdom, the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017)
- the identity of the directors and persons responsible for the management of the agent and, if the agent is not a payment service provider, evidence that they are fit and proper persons
- the payment services for which the agent is appointed
- the unique identification code or number of the agent, if any
- any other information which we reasonably require

Name and address details

5.12 We require details of the PI or EMI and its agent so we can identify both parties and meet our supervisory and registration requirements.

AML internal control mechanisms

5.13 The PI or EMI should demonstrate that it has and maintains appropriate and risk-sensitive policies and procedures for countering the risk that it, or its agents, may be used to further financial crime.

5.14 We require a description of the internal control mechanisms that will be used to comply with the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 and other pieces of financial crime legislation. Where agents are based in another EEA state, authorised PIs or EMIs must ensure the anti-

money laundering systems and controls comply with local legislation and regulation that implements Directive (EU) 2015/849 and that such requirements are followed by their agents.

5.15 The description of internal control mechanisms only needs to be supplied once if a PI or EMI applies the same controls to all its agents and it has not changed from previous appointments. If the PI or EMI has previously supplied this information they should indicate this on the agent application form. The PI or EMI must provide an updated version of its internal control mechanisms without undue delay if there are significant changes to the details communicated at the initial notification stage.

5.16 PIs and EMIs should take reasonable measures to satisfy themselves that the agents' anti-money laundering internal controls mechanisms remain appropriate throughout the agency relationship.

Directors and persons responsible for the management of the agent

5.17 Regulation 34(3) of the PSRs 2017 and regulation 34(3) of the EMRs require that the application to register an agent must also provide:

- the identity of the directors and persons responsible for the management of the agent
- if the agent is not a payment service provider, evidence that they are fit and proper persons

5.18 We must be provided with details of the director(s) and persons responsible for the management of the agent. For incorporated agents this is the board members, or for unincorporated agents the partners or sole trader, together with any other person that has day-to-day responsibility for the management of the agent.

5.19 To verify identity, we require the name, national insurance number for UK residents (or taxation insurance number for non-UK residents) and date and place of birth for each person.

5.20 Where the agent is not itself a payments service provider (for example a PI or EMI) we also need evidence that the individuals are fit and proper persons. EMIs and PIs should carry out their own fitness and propriety checks on their agents, on the basis of a 'due and diligent' enquiry before completing the application form to register an agent. The assessment should be proportionate to the nature, complexity and scale of risk in the distribution, redemption, payment services or other activities being carried out by the agent.

5.21 We expect PIs or EMIs to consider the following factors when making enquiries about the fitness and propriety of the directors and persons responsible for the management of an agent of a PI or EMI:

- honesty, integrity and reputation
- competence and capability
- financial soundness

5.22 For more information on the types of enquiries we expect PIs and EMIs to make when gathering information about these factors, please see the information on the fit and proper assessment in **Chapter 3 – Authorisation and registration**, especially in 3.67.

5.23 The PI or EMI must certify that the individuals are fit and proper and disclose any adverse information. We will use the enquiries made by the PI or EMI to help our assessment of these matters.

Payment services for which agent is appointed

5.24 For agents of both PIs and EMIs we require details of the payment services which the agent has been appointed to provide.

Unique identification code or number

5.25 We will, where applicable, require details of the unique identification code or number of the agent. For UK agents, this is the Firm Reference Number (where it is already on the Financial Services Register) as well as its Companies House registration number or, for unincorporated agents, the national insurance number(s) of those involved in the management of the agent. If the UK agent has a Legal Entity Identifier[9] (LEI) this must also be provided. For EEA agents an LEI or another identification number, as specified in Annex 1 of the European Banking Authority's Regulatory Technical Standards on the framework for cooperation and exchange of information between competent authorities for passport notifications under Directive (EU) 2015/2366 should be provided.[10] Also see **Chapter 6 – Passporting** on passporting activities.

Additional information and changes to information supplied

5.26 At any time after receiving an application and before determining it, we may require the applicant to provide us with further information as we consider reasonably necessary to determine their application (regulation 34(5) of the PSRs 2017 and regulation 34(5) of the EMRs). This can include documents to support the fitness and propriety checks carried out on agents.

5.27 Once an application has been submitted, before it has been determined and on an ongoing basis, applicants must tell us about significant changes in circumstances relating to the fitness and propriety of an agent's management or of anything relating to money laundering or terrorist financing without undue delay.

Decision making

5.28 We are required to make a decision on registering an agent within two months of receiving a complete application where the agent is engaged in relation to the provision of payment services or e-money issuance in the UK.

---

[9] An LEI is a unique identifier for persons that are legal entities or structures including companies, charities and trusts. Further information on LEIs, including answers to frequently asked questions, can be found on the Legal Entity Identifier Regulatory Oversight Committee and Global Legal Entity Identifier Foundation websites.

[10] These RTS are available here: https://www.eba.europa.eu/-/eba-publishes-final-draft-technical-standards-on-cooperation-and-exchange-of-information-for-passporting-under-psd2.

5.29 With services provided through an EEA agent using passporting rights, our decision will take into account information given to us by the host state competent authority (See **Chapter 6 - Passporting**). We are required to make a decision on EEA agent registration within three months of receiving a complete application.

Approval

5.30 We update the register when we approve an agent application, usually within one business day. We also communicate the application result to the PI or EMI. If, after two months or, for an agent in another EEA Member State, three months (see **Chapter 6 - Passporting**), the agent does not appear on the register, the PI or EMI should contact the Customer Contact Centre. PIs and EMIs cannot provide payment services through an agent until the agent is included on the register.

5.31 Under regulation 34(14) of the PSRs 2017 and regulation [TBC] of the EMRs, PIs must notify the FCA of the date when they start to provide payment services in another EEA State through a registered EEA agent. PIs should notify us using the FCA Connect System. EMIs should notify us using the relevant form on the e-money section of our website. The FCA must notify such date to the relevant host state competent authority.

Refusal

5.32 The PSRs 2017 and the EMRs only allow us to refuse to include the agent in the register where:

- we have not received all the information required in the application (see **Making an application** above) or we are not satisfied that the information is correct
- we are not satisfied that the directors and persons responsible for the management of the agent are fit and proper persons
- we have reasonable grounds to suspect that, in connection with the provision of services through the agent
  - money laundering or terrorist financing within the meaning of the Money Laundering Directive (or Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 in the UK) is taking place, has taken place or been attempted
  - the provision of services through the agent could increase the risk of money laundering or terrorist financing

5.33 Where the application relates to the provision of payment services in exercise of passport rights through an EEA agent, we will take into account any information received from the host state competent authority and notify the host state competent authority of our decision, providing reasons if we do not agree with their assessment.

5.34 **Chapter 14 – Enforcement** provides more information on what we will do if we propose to refuse to include an agent on our Register.

Cancellation of agents

5.35 To cancel an agent registration the principal must submit a *Remove PSD agent* application through the FCA Connect system or complete the *Remove EMD agent* form, which is available on the e-money section of our website. We will update the register to show that the agent is no longer registered to act for the principal once we have finished processing the notification.

5.36 If an agent is being used to perform payment services in another EEA State, the principal may also need to amend the details of the passport, and must submit a *Change in passport details* application through the FCA Connect system (for PIs) or fill in the *Change in passport details* form (for EMIs) (see **Chapter 6 - Passporting**). Please note that if a PI or EMI removes its last EEA agent within one EEA member state, the relevant PSD or EMD establishment passport must be cancelled.

Changes to agent details

5.37 The principal must submit an *Amend PSD agent* application through the FCA Connect system (for PIs) or use the *Amend EMD agent* form which is available on the e-money section of our website (for EMIs), to amend the details of an agent.

5.38 We will assess the impact of the change against the agent registration requirements. If the change is approved we will update the register as soon as possible. If we need more information we will contact the payment service provider, and if the change is not approved we will follow the refusal process set out above.

Notifying HMRC

5.39 The PI or EMI should make sure that HMRC's Money Service Business Register is up to date and that any agent submissions made to us have been included in the list of premises notified to HMRC.

6. Passporting

6.1 This chapter describes the process that authorised PIs and authorised EMIs will need to go through if they wish to provide payment services or, in the case of authorised EMIs, issue, distribute or redeem e-money in another EEA State. It also tells PIs and EMIs authorised in another EEA State how we will deal with notifications to provide payment services or issue, distribute or redeem e-money in the UK that we receive from their home state regulator.

6.2 The EBA has issued regulatory technical standards specifying the method, means and details of the cross-border cooperation between competent authorities in the context of passporting notifications ('Passporting RTS').[11] [Once published in the Official Journal of the European Union, the Passporting RTS will become a Commission Delegated Regulation. To be updated once this has occurred.] This chapter should be read alongside the Passporting RTS.

Introduction

6.3 Passporting is the exercise of the right of an authorised firm to conduct activities and services regulated under EU legislation in another EEA State on the basis of authorisation in its home member state. The activities can be conducted through an establishment in the host state (known as a 'branch' passport) or on a cross-border services basis without using an establishment in the host state (a 'services' passport). A physical presence established in another member state by a UK authorised PI or UK authorised EMI is referred to as an 'EEA branch' (see Q45 in PERG 15.6 for further guidance). Regulations 26 to 30 of the PSRs 2017 and 28 to 30 of the EMRs set out the respective procedures for the exercise of passporting rights by authorised PIs and authorised EMIs.

6.4 Passporting rights are only available to authorised PIs (and RAISPs; see below) and authorised EMIs (except authorised EMIs whose head office is situated outside the EEA), not small PIs or small EMIs.

Authorised PIs

6.5 The passporting right extends to all the payment services for which the authorised PI is authorised but does not, in our view, extend to other activities that authorised PIs may perform that are ancillary to the provision of payment services (see regulation 32 PSRs 2017). Whether an authorised PI can carry on those other activities in another EEA State will depend on the local law in that state and firms may therefore wish to take professional advice if they think their business is likely to be affected by this.

6.6 A UK authorised PI can also provide services in another EEA State through an agent established in the UK (using a 'services' passport) or in another EEA State (using its right of establishment). In this chapter we refer to such an agent, and the agent of an EMI, as an 'EEA agent'.

[11] The Passporting RTS are available here: https://www.eba.europa.eu/-/eba-publishes-final-draft-technical-standards-on-cooperation-and-exchange-of-information-for-passporting-under-psd2.

6.7 PSD2 introduces two new payment services that can be passported: PIS and AIS (described in more detail in **Chapter 17 – Payment initiation and account information services and confirmation of availability of funds**) and a new type of firm - the RAISP.

6.8 Under regulation 26 of the PSRs 2017, RAISPs are treated as if they are authorised PIs for the purposes of the passporting provisions in regulations 27 – 30. As such, RAISPs are permitted to exercise their right to passport in respect of AIS. It should be noted that the activity of executing 'payment transactions where the consent of the payer to execute a payment transaction is given by means of any telecommunication, digital or IT device and the payment is made to the telecommunication, IT system or network operator acting only as an intermediary between the payment service user and the supplier of the goods or services' will, subject to the application of the transitional provisions in the PSRs 2017, no longer exist under PSD2.

Authorised EMIs

6.9 A UK authorised EMI can provide payment services in another EEA state through an agent established in the UK or an agent established in another EEA state, subject to the requirements in the EMRs. A UK authorised EMI may also engage an agent or a distributor to distribute or redeem e-money in another EEA state in the exercise of its passport rights. An EMI may not, however, issue e-money through a distributor or an agent.

6.10 Where an authorised EMI wishes to distribute or redeem e-money in another EEA state by engaging one or more distributors, it must follow the normal notification procedures – that is to say those applicable to agents under a service or establishment passport – and provide us with a list of all distributors, including name, address and (in the case of natural persons) date and place of birth, together with other information requested. We will then communicate this information to the host state competent authority.

Further guidance

6.11 PERG 15.6 and Chapter 3A of our Perimeter Guidance (PERG) provide further guidance on when we consider a passport notification needs to be made by an authorised PI and authorised EMI respectively. The passporting section of our website includes answers to frequently asked questions with regard to both authorised PIs and authorised EMIs.

Making a passport application

6.12 The procedures for making an application to exercise passport rights differ depending on the precise way in which the authorised PI or authorised EMI wishes to carry on payment services in another EEA State.

- The Passporting RTS distinguish between
  (1) branch passport notifications by authorised PIs and authorised EMIs
  (2) passport notifications by authorised PIs and authorised EMIs using agents

(3) passport notifications by authorised EMIs using distributors
(4) services passport notifications with no agent or distributor.

We have reflected these categories of passporting notification in our passporting forms. The procedures for all types of passport application are set out below.

Notice of intention

6.13 Where an authorised PI or authorised EMI intends to provide payment services or, in the case of an authorised EMI, issue, distribute or redeem e-money, into another EEA state, either on a freedom of services or establishment basis, regulation 27 of the PSRs 2017 and regulation 28 of the EMRs (as applicable) requires the firm to submit a notice of intention to passport through the FCA Connect system.

6.14 Our notice of intention forms reproduce the notification templates set out in the annexes to the Passporting RTS through which we are required to transmit information and cover passport applications by:

- authorised PIs and authorised EMIs in relation to the freedom to provide services with no agent or distributor;
- authorised PIs and authorised EMIs in relation to a branch;
- authorised PIs and authorised EMIs using agents; and
- authorised EMIs using distributors.

6.15 The notice of intention for all passport applications must include the name, address and authorisation or reference number of the firm, the payment services and / or e-money services that it intends to carry on, and the EEA state(s) where the services are to be performed. Specific information related to the nature of the passport application will also be required and is set out below in more detail.

6.16 The requirement to provide an authorisation or reference number can be satisfied in a number of ways. As part of the passport application, authorised PIs and authorised EMIs will be asked for the following:

- unique identification number, which is the firm's tax number (but note that this is just for UK firms)
- Legal Entity Identifier (LEI) which is a unique globally recognised code, issued under these arrangements: https://www.leiroc.org. We appreciate that many firms will not have an LEI so it will only need to be provided where available,
- home state authorisation number which will be the firm's FCA firm reference number

6.17 We are required to assess the completeness and accuracy of the information provided in all payment applications we receive. Where the information is deemed not to be complete or to be incorrect, we will inform authorised PIs and authorised EMIs without delay.

Notification process

6.18 Once we have received a complete application, we will check that the services the applicant intends to provide in the host state are within the scope of its UK authorised activities.

6.19 In accordance with Regulation 27(3) of the PSRs 2017, we will transmit the information to the host member competent authority within one month of receipt of a complete and accurate passport application. As this time period will not commence until all information has been received, we would encourage all firms to ensure that the information provided is as accurate as possible on first submission to avoid delays in the passporting approval process. We will inform you that the information has been sent.

6.20 The date on which we receive a complete application will form part of the information that we transmit to the host state competent authority.

6.21 Under PSD2, the host state competent authority will then have another month in which to assess the information and inform us of anything which may be relevant to the intended provision of payment or e-money services under the passport. This applies to applications under both the right of establishment and the freedom to provide services (see section 6.40 for more details on the assessment of information received from host state competent authorities).

6.22 PSD2 also requires us to communicate our decision on whether authorised PIs and authorised EMIs are permitted to passport their services before they can commence activities in another EEA state. If we are minded to reject an application, we must give a warning notice, the responses to which will assist us in making our decision. In any event, the decision to grant or reject the application must be communicated to both the firm and the relevant competent authority in the host state.

6.23 We must provide our decision within three months of receipt of the notification (again dated from receipt of "complete" information). EEA agents and branches are also only permitted to commence their activities in a host member state once they are entered on the Financial Services Register. Authorised PIs and authorised EMIs should therefore not undertake any activity - either cross border or through a branch, EEA agent or distributor - until our decision has been notified to them (and the host state competent authority) and they appear on the FS Register. In accordance with the requirements of the Passporting RTS and Article 28(3) of PSD2, authorised PIs and authorised EMIs should assume that all passport applications will take three months from receipt of complete and correct information by the FCA. In practice, this timescale may be shorter for firms applying for a services passport or in circumstances where host state competent authorities revert to the FCA before the end of the time permitted under PSD2.

6.24 Authorised PIs and authorised EMIs are required to notify us of the date on which they commence their activities in another EEA state through a branch, agent or distributor. We will then inform the relevant EEA state regulator accordingly.

Service passports – not involving an EEA agent or distributor

6.25 Authorised PIs and authorised EMIs wishing to provide cross border services must submit the relevant notice of intention through Connect.

6.26 In addition to the general information required in all passport applications (see section 6.15), notifications for services passports sent to host state competent authorities must also include details such as:

- the name, email and telephone number of the contact person within the authorised PI or authorised EMI,
- the intended start date from which payment or e-money services will be provided and
- details of any outsourcing of operational functions related to the provision of payment or e-money services.

Branch (or establishment) passports

6.27 Authorised PIs and authorised EMIs wishing to provide services through the use of a branch will have to submit the relevant notification through Connect.

6.28 In addition to the general information required in all passport applications (see section 6.15), notifications for branch passports sent to host state competent authorities must also include details such as:

- the address of the proposed branch, the name, email and telephone number of the people responsible for managing the branch,
- a description of the organisational structure of the branch as well as
- a business plan demonstrating that the branch will be able to employ the appropriate and proportionate systems,
- resources and procedures to operate soundly in the host Member state
- a description of the governance arrangements and internal control mechanisms of the branch
- and of any outsourcing of operational functions related to the provision of payment or e-money services.

Use of EEA agents and distributors

6.29 Under PSD2, authorised PIs and authorised EMIs wishing to provide payment services in other EEA states through the use of agents may do so under either an establishment or freedom to provide services passport. The same applies to EMIs using distributors.

6.30 A firm that considers it would be exercising the freedom to provide services, rather than the freedom of establishment, in passporting using an agent or distributor must explain the circumstances that form the basis of that view. We will be required to make an assessment of which type of passport is appropriate for applicants when making our notifications to host state competent authorities. In circumstances where agree with the

applicant firm that a services passport is appropriate, we will be obliged to state the reasons for this decision in the notification.

6.31 The application processes for passports using EEA agents and distributors are very similar. As with applications for the branch and services passports, firms will be required to provide the general information set out in section 6.15 above. In both cases, firms will also be required to provide the following additional information:

- whether the application is for a branch, establishment or services passport
- a description of the internal control mechanisms that will be used in order to comply with the obligations in relation to money and terrorist financing
- details of outsourcing arrangements for operational functions of payment or e-money services
- if the agent / distributor is a natural person:
    - name, date and place of birth of the individual
    - unique identification number of the agent
    - telephone number and email of the agent
- if the agent / distributor is a legal entity:
    - unique identification number
    - legal entity identifier (LEI) (where available)
    - telephone number and email
    - name, place and date of birth of its legal representatives

6.32 Authorised PIs and authorised EMIs wishing to use EEA agents have further information requirements that cover the identity and contact details of directors and persons responsible for the management of the agent to be used and, for agents other than payment service providers (i.e. those without authorisation in their own right) evidence that the directors and management are fit and proper persons (please see section 6.35 below).

6.33 Where firms are operating through agents on a branch / establishment basis in another EEA state, the host state competent authority will have the right to require them to appoint a central contact point in that state under Article 29(4) of PSD2. In these circumstances, firms must provide details of this central contact point, i.e. name, address, telephone number and email.

Fitness and Propriety

6.34 Where a firm seeks to establish a branch, or provide services through an EEA agent or distributor (either exercising its right of establishment or using a services passport), we are required to assess the fitness and propriety of the management of the branch/EEA agent or distributor and, as part of this, we are required to make a notification to the host state competent authority. We must take the host state competent authority's opinion on certain matters into account.

6.35 The appointment of an EEA agent or distributor by an authorised PI or authorised EMI is subject to the directors and persons responsible for the management of the agent / distributor being fit and proper. As per **Chapter 5 – Appointment of Agents**, the authorised PI or authorised EMI should carry out its own fitness and propriety review

of its proposed agents and distributors before completing the application form to register an EEA agent / distributor. We will use the enquiries made on these persons to help our assessment of these matters. Under regulation 34(3)(a)(iii) of the PSRs 2017, the authorised PI or authorised EMI has to provide the FCA with evidence that the directors and persons responsible for the management of the agent are fit and proper persons. We may also require the applicant firm to provide us with such further information as we reasonably consider necessary to enable us to determine the application.

6.36 If we assess the information in the application to be complete and correct, we will make the notification to the relevant host state competent authority that we are proposing to include the EEA agent on our register. As mentioned above, we are required to make this notification within one month of receipt of a complete notification and host state competent authorities have another month in which to assess the information provided.

6.37 Under Article 28(2) of PSD2, host state competent authorities are required to inform us in particular of any 'reasonable grounds for concern in connection with the intended engagement of an agent or establishment of a branch with regard to money laundering or terrorist financing'.

6.38 We are entitled to disagree with any assessment made by a host state competent authority and will be required to explain our reasons for doing so. If our assessment of the information they provide is unfavourable to the applicant, we will be required to refuse to register the EEA agent, branch or distributor and either ask the firm to withdraw the application or take steps to cancel any application already made.

6.39 As explained above, authorised PIs and authorised EMIs should assume that all passport applications will take three months from receipt of complete and correct information by the FCA. In practice, this timescale may be shorter for firms applying for a services passport or in circumstances where host state competent authorities revert to the FCA before the end of the time permitted under PSD2.

6.40 We continue to expect a high turnover of EEA agents, therefore to keep down the costs to firms we will not acknowledge notifications of changes in EEA agents. If we are not satisfied or, if in response to our notification to the EEA host state competent authority, we receive information that changes our initial view, the refusal process followed will be the same as outlined in **Chapter 3 – Authorisation and registration**. If an EEA agent is being added to an existing passport, then in accordance with our policy on the appointment of agents, firms should, where necessary, check the register to confirm that the agent has been registered. Firms should check our website for expected turnaround times, and contact the Customer Contact Centre if the agent does not appear within the expected period.

6.41 In addition to the power to refuse registration, we can cancel existing registrations of branches under regulation 28(1) of the PSRs 2017 and 29(1) of the EMRs and of EEA agents under regulation 35(1) of both the PSRs 2017 and the EMRs. We also have powers under regulation 7 of both the PSRs 2017 and EMRs to impose requirements on the authorised PI's and authorised EMI's authorisation. If we decide not to approve the passport notification as requested by the firm, we will follow a decision making process equivalent to that described in Part III, **Chapter 3 – Authorisation and registration**.

Making changes

6.42 Changes that affect the services that an authorised PI or authorised EMI seeks to carry on under passporting rights should be notified to us at least one month before firms wish them to take effect. Such changes cover all information provided in the initial notification and may include:

- changes to the name or address of the firm, or agent engaged in another member state;
- adding/removing an agent or distributor;
- adding/removing passporting rights to particular EEA states;
- changes to the payment services being conducted;
- changes to the persons responsible for the management of the proposed EEA branch or EEA agent; or
- changes to the organisational structure or governance arrangements of the branch or agent.

6.43 A notification of changes will be subject to a similar review process as a new passport notification where it involves a change to the structure of the establishment. For example, a change in the agents being used or the individuals responsible for managing an establishment may be subject to the fitness and propriety checks and require an updated organisational structure to be submitted to reflect the changes to be made.

Incoming EEA authorised PIs and EMIs

6.44 PIs and EMIs that are authorised in another EEA State that wish to provide payment services in the UK ('EEA-authorised PIs') or wish to issue, distribute or redeem e-money or provide payment services in the UK should refer to the competent authority in their home state for instructions on making a passport notification. These authorised EMIs (EEA-authorised EMIs) and EEA authorised PIs will appear on the register of their home state, but not our FS register.

6.45 When we receive a passport notification from the home state's competent authority in respect of an authorised PI or authorised EMI intending to establish a branch in the UK or use a UK agent or distributor, we are entitled to review the notification for any relevant matters, especially relating to suspicions of money laundering and terrorist financing involvement as outlined above. Where we have concerns, we will notify the home state competent authority within one month of receipt of the notification; the home state competent authority will then have one month to decide what action to take.

6.46 Changes to an EEA authorised PI's or EEA authorised EMI's passport should be notified to its home state's competent authority who will notify us, as appropriate.

6.47 In our view, an EEA authorised PI's or EEA authorised EMI's passport entitles it to carry on in the UK only payment services or issuing, distributing and redeeming e-money and payment services notified to us by the home state competent authority, respectively.

6.48 If an EEA authorised PI or EEA authorised EMI wishes to carry on other activities in the UK, it may need to seek other appropriate authorisation, registration or make use of another passport (for example, to provide investment services under the Markets in Financial Instruments Directive (MiFID)).

Supervision of incoming EEA PIs and EMIs

6.49 We are responsible for supervising compliance by an FCA-authorised PI or FCA-authorised EMI with its capital requirements obligations, regardless of where it carries on its payment services within the EEA, but we are not responsible for supervising compliance with capital requirements by an EEA authorised PI or EEA authorised EMI authorised in another member state.

6.50 We are responsible for supervising compliance with the conduct of business requirements of the PSRs 2017 / EMRs in relation to payment services and e-money services being provided from an establishment in the UK (for example, by an EEA authorised PI or EEA authorised EMI exercising its right of establishment), but not in relation to those provided on a cross-border basis from an establishment outside the UK (for example, under a services passport).

6.51 Under Regulation 30 of the PSRs 2017, we may require an EEA authorised PI that exercises its right to passport through a branch or agent in UK to report to us on its activities. Firms that operate through agents in the UK under the right of establishment may also be required to appoint, and provide us with contact details for, a central contact point in the UK. There are RTS developed by the EBA under article 29 (5) of PSD2 specifying the criteria to be applied when determining the circumstances when the appointment of a central contact point is appropriate and the functions of those contact points.

6.52 We will exchange information about authorised PIs and authorised EMIs and EEA authorised PIs and EEA authorised EMIs with other competent authorities in accordance with the PSRs 2017 and EMRs (as applicable) and both the Passporting RTS and the RTS developed by the EBA under article 29(6) of PSD2 specifying the means of monitoring compliance with the provisions of national law transposing PSD2 and the exchange of information between home and host state competent authorities. In particular, we are obliged to provide relevant competent authorities with all relevant or essential information relating to the exercise of passport rights by an authorised PI or authorised EMI, including information on breaches or suspected breaches of the PSRs 2017 / EMRs and of money laundering and terrorist financing legislation.

7. Status disclosure and use of the FCA logo

7.1 This chapter explains what PIs and EMIs may say about their regulatory status and the restriction on the use of the FCA logo.

7.2 We have decided not to allow any firm to use the FCA logo in any circumstances. Our reasons are set out in FSA Policy Statement 13/5 of March 2013 at section 2.3 and incorporated into the FCA Handbook in Chapter 5 of the General Provisions Chapter (GEN 5).

7.3 This does not prevent any PI, EMI or RAISP from making a factual statement about its regulatory status (as is required in the information requirements in Part 6 of the PSRs). **Annex 3** sets out some sample statements for PIs, EMIs and RAISPs to describe their regulatory relationship with us.

8. Conduct of business requirements

8.1 This chapter describes the conduct of business requirements. The PSR conduct requirements apply to all PSPs — including EMIs when providing payment services — except credit unions, municipal banks and the National Savings Bank. The EMR conduct requirements apply to all e-money issuers.

8.2 The chapter is set out as follows:

- introduction, application and interaction with other legislation
- Part I: Information requirements:
  - A – framework contracts
  - B – single payment transactions
  - C – other information provisions
- Part II: Rights and obligations
- Part III: Additional conduct of business requirements for e-money issuers.

Introduction

8.3 Parts 6 and 7 of the PSRs 2017 set out obligations on PSPs relating to the conduct of business in providing payment services. These are typically referred to as 'conduct of business requirements'.

8.4 They fall into two main categories:

- information to be provided to the customer before and after execution of a payment transaction
- the rights and obligations of both PSP and customer in relation to payment transactions

8.5 The information requirements differ depending on whether the transaction concerned is carried out as part of an ongoing relationship under a 'framework contract' or as a single payment transaction. There are also different requirements for payment instruments that are limited to low value transactions.

8.6 Customers that are larger businesses can, in some cases agree with their PSP that certain provisions of the PSRs 2017 will not apply. This is known as the "corporate opt out". We identify throughout this chapter where the corporate opt out can be used. The corporate opt out can only be used where the customer is not:

- a consumer
- a micro-enterprise (see [Glossary] for definition)
- a charity with an annual income of less than £1 million

8.7 It is important to note that the PSRs 2017 provide that the agreement may be that "any or all of [the relevant regulations] do not apply". In our view it must be made clear to the customer which provisions are being disapplied. The PSRs 2017 contain an

overarching provision allowing PSPs to offer more advantageous terms to their customers than those set down in the PSRs 2017.

8.8 Definitions for the terms used in this chapter can be found in regulation 2 of the PSRs 2017.

Application of the conduct of business requirements

8.9 The conduct requirements in the PSRs 2017 apply to payment services provided from an establishment in the UK, irrespective of the location of any other PSP involved or the currency of the transaction. However, there are exceptions to this.

8.10 Where one of the PSPs is located outside the EEA, Parts 6 and 7 of the PSRs 2017 apply only to the parts of a transaction which are carried out in the EEA. Certain requirements only apply to transactions where the PSPs of both the payer and the payee are located in the EEA or where the payment transaction is in euro, or the currency of a member state that has not adopted the euro.

8.11 We have added guidance in **Chapter 2 - Scope** to assist PSPs with establishing whether a particular conduct of business requirement applies to a payment service/transaction.

Interaction with other legislation

8.12 In addition to complying with the PSRs 2017, PSPs will need to comply with other relevant legislation.

FSMA and the FCA Handbook

8.13 Firms which are regulated under FSMA (for example, because they are accepting deposits, carrying on credit-related regulated activities or regulated investment business) must comply with relevant obligations in the Handbook. For example, where applicable, they must comply with the Principles for Businesses as long as these do not conflict with the PSRs 2017 or EMRs.

8.14 We describe below some other Handbook and legislative requirements that FSMA authorised firms may need to take into account.

Consumer Credit Act 1974 (CCA) and CONC

8.15 Generally speaking**,** businesses that lend money to retail consumers are required to be authorised by us unless they are exempt or an exclusion applies.

8.16 The Consumer Credit sourcebook (CONC) sets out the detailed obligations that are specific to credit-related regulated activities and activities connected to those credit-related regulated activities carried on by firms. Other conduct of business requirements are imposed by the Consumer Credit Act 1974 (CCA) and legislation made under it.

8.17 Under regulation 32(2) of the PSRs 2017, PIs and under regulation 32(2) of the EMRs, EMIs may grant credit, subject to the conditions outlined in regulation 32(2) of the PSRs 2017 [and the EMRs] which include that the credit is not granted from the funds received or held for the purposes of executing payment transactions or in exchange for

e-money. Where the granting of the credit is regulated by FSMA, the firm is also required to have authorisation under that Act.

8.18 If a PSP grants credit, the general principle is that, where a PSP provides a payment service and grants credit, the two regulatory regimes apply cumulatively. However, there are some exceptions to this and the PSP needs to be aware of how the two regimes interact. We set out more detail in paragraphs 8.59 – 8.63.

The Banking: Conduct of Business sourcebook (BCOBS)

8.19 Retail deposit takers, — e.g. banks, building societies and credit unions — are required to comply with BCOBS.

8.20 Broadly speaking, BCOBS does not apply where conduct in relation to a service is already regulated under the PSRs 2017. Chapter 1 of BCOBS sets out which provisions of BCOBS apply cumulatively to payment services alongside Parts 6 and 7 of the PSRs 2017 (e.g. BCOBS 2 in relation to communications and financial promotions and BCOBS 6 relating to cancellation) and which provisions of BCOBS do not apply to payment services where Parts 6 and 7 of the PSRs 2017 apply (eg most of BCOBS 4 relating to information requirements).

8.21 For payment accounts provided by banks and building societies in connection with accepting deposits, the provisions in Parts 6 and 7 of the PSRs 2017 about the disclosure of specified items of information at the pre-contract and post contract stages, liability for unauthorised payments, execution of payments and security and authentication of payments will always apply. This means that the corresponding provisions of BCOBS that regulate the same matters do not apply.

8.22 For provision of accounts that are not payment accounts (for example some savings accounts) the requirements in Parts 6 and 7 of the PSRs 2017 do not generally apply, and so BCOBS will apply to the retail banking service. The effect of this is, for example, that if a PSP wishes to change the interest rates on an account which is not a payment account, the PSP will need to apply the relevant notice period under BCOBS, not the PSRs 2017.

8.23 The PSRs 2017 do apply to payment transactions within the scope of the PSRs 2017 that are made to and from such accounts. This means, for example, that the PSR information requirements must be complied with in relation to such transactions, and if the PSP failed to execute a transaction from such an account correctly, regulations 91 and 92 of the PSRs 2017 would apply because the PSRs 2017 apply to that payment transaction. Guidance on the meaning of payment account is set out in PERG 15.

8.24 Because credit unions are exempt from the PSRs 2017, the conduct provisions of BCOBS will apply to them in respect of their retail banking services, except where expressly disapplied (see BCOBS 1.1.5R).

8.25 BCOBS includes rules relating to:

- communications with banking customers and financial promotions
- distance communications, including the requirements of the Distance Marketing Directive and E-commerce Directive
- information to be communicated to banking customers, including appropriate information and statements of account
- post-sale requirements on prompt, efficient and fair service, moving accounts, and lost or dormant accounts
- cancellation, including the right to cancel and the effects of cancellation

The BCOBS sourcebook.

Other Legislation

Distance Marketing Directive

8.26 The Distance Marketing Directive (DMD) provides protection for consumers whenever they enter into a financial services contract by distance means, including for payment services. Both the PSRs 2017 and the DMD apply to contracts for payment services. In particular, PSPs should be aware of the information requirements in the DMD which apply in addition to the information requirements in the PSRs 2017.

8.27 The rules implementing the DMD in relation to retail banking services can be found in BCOBS. For PSPs and e-money issuers that are not undertaking a FSMA regulated activity, the rules implementing the DMD are found in the Financial Services (Distance Marketing) Regulations 2004 ("DMRs") and, for regulated credit agreements, they are found in CONC.

Cross-border payments and Single Euro Payments Area (SEPA) legislation

8.28 Regulation 924/2009 is a directly applicable EU regulation that prohibits PSPs from charging more for a cross-border payment in euro, Swedish kronor or Romanian lei than for a corresponding domestic payment in the same currency. The FCA is the competent authority and the FOS is the out-of-court redress provider for this regulation.

8.29 Regulation 260/2012 (SEPA Regulation) lays down rules for credit transfer and direct debit transactions in euro where both the payer's PSP and the payee's PSP are located in the EEA, or where the sole PSP in the payment transaction is located in the EEA. The SEPA Regulation is also directly applicable, and the FCA is the UK competent authority.

The E-Commerce Directive (2000/31/EC)

8.30 The E-Commerce Directive establishes harmonised rules on issues such as the transparency and information requirements for online service providers, commercial communications and electronic contracts.

8.31 The rules implementing the E-Commerce Directive in relation to deposit-taking and activities associated with that activity can be found in the Handbook in BCOBS 3.2. For credit-related regulated activity, the rules implementing the E-Commerce Directive can be found in CONC 2.8.

8.32 For other payment services and issuance of e-money, the rules implementing the E-Commerce Directive are found in the Electronic Commerce (EC Directive) Regulations

2002.

Unfair Contract Terms - The Unfair Terms in Consumer Contracts Regulations 1999 (UTCCRs) and the Consumer Rights Act 2015 (CRA)

8.33 The CRA applies to contracts between consumers and PSPs or e-money issuers entered into on or after 1 October 2015 (the UTCCRs continue to apply to contracts concluded before that date).

8.34 The CRA requires terms used by businesses in their contracts and notices to be fair. Further information about the CRA and UTCCRs can be found in The Unfair Terms and Consumer Notices Regulatory Guide (UNFCOG), on our website and on the CMA website. PSPs and e-money issuers must ensure that their consumer contracts comply with both the conduct of business provisions of the PSRs 2017 and EMRs and the unfair contract terms provisions of the CRA (or UTCCRs).

The Consumer Protection from Unfair Trading Regulations 2008 (CPRs)

8.35 PSPs and e-money issuers should note that the CPRs apply to their payment service and e-money business with consumers. The CPRs are intended to protect consumers from unfair commercial practices by businesses. "Commercial practices" include advertising and marketing or other commercial communications directly connected with the sale, promotion or supply of a product. Further information about the CPRs can be found on our website. The CMA has also published guidance relating to the CPRs.

8.36 In providing customers with details of their service, providers and e-money issuers must avoid giving customers misleading impressions or marketing in a misleading way. For example:

- misleading as to the extent of the protection given by safeguarding
- suggesting funds are protected by the Financial Services Compensation Scheme, or displaying the FSCS logo
- misleading as to the extent of FCA regulation of unregulated parts of the business
- describing accounts that are provided by PSPs that are not credit institutions as 'bank accounts' or 'banking services'
- advertising interbank exchange rates that will not be available to the majority of customers
- advertising material or business stationery that is likely to mislead customers in these areas may potentially constitute a misleading commercial practice under the CPRs

8.37 Where a money transfer operator PI operates as a 'wholesaler' (providing a payment service to smaller money transfer operators, but without a contractual relationship with the payment service user) and provides its client PIs with advertising materials and stationery, the use of such material must be compatible with the CPRs.

8.38 Advertising material or business stationery that is likely to mislead customers into believing that the PSP with whom they have contracted is the wholesaler rather than the client may potentially constitute a misleading commercial practice under the CPR. In these circumstances it is unlikely that simply referring to the client's name on the customer's receipt will, in itself be sufficient to achieve compliance, as this occurs after

the transaction has been entered into. Where it appears to us that a PSP's business model has changed from an agency to a wholesaler model purely as a matter of form rather than substance, in order to avoid its regulatory obligations for its agents, this is seen as a matter of concern.

8.39 The FCA is able to enforce the CPRs as a "designated enforcer" through Part 8 of the Enterprise Act 2002.

The Payment Account Regulations 2015 (PARs)

8.40 The PARs, which implement the Payment Accounts Directive, introduced greater transparency of fees and charges, easier account switching and better access to basic bank accounts.

8.41 The requirements of the PARs apply vis-a-vis consumers, whereas the requirements of the PSRs 2017 apply vis-a-vis all payment service users (which includes business customers).

8.42 The PARs apply to "payment accounts" but they have their own definition of this, which is narrower than the definition of "payment account" under the PSRs 2017. This means that some accounts will be classed as "payment accounts" under the PSRs 2017, but won't be classed as 'payment accounts' under the PARs (for example, certain savings accounts). PSPs should be careful to apply the correct definition of "payment account" depending on which regime they are applying.

8.43 Where both the provisions in the PARs and the PSRs 2017 apply to accounts, PSPs must comply with both sets of requirements. For example, the PSRs 2017 require charges information to be provided to customers pre-contractually. The PARs will require a fee information document to be provided pre-contractually. The requirement under the PARs applies in addition to the requirements in the PSRs 2017 (see regulation 8(1)(a) of the PARs). However, PSPs could use the fee information document to provide details of charges under the PSRs 2017, provided the requirements of both pieces of legislation are met.

8.44 Similarly, where the provisions in the PARs and the PSRs 2017 apply to a basic bank account, regulation 51 of the PSRs 2017 will apply to the termination of the account. However, this is subject to the specific list of termination conditions set out in regulation 26(1) of the PARs which limit the reasons that a payment account with basic features can be terminated by the PSP.

8.45 Further guidance on the PARs can be found on the FCA website.

ISA Regulations and COBS

8.46 Where PSPs are providing ISAs, they also need to be aware of their obligations under the ISA Regulations and the Conduct of Business Sourcebook in the Handbook.

The Directive on security of network and information systems

8.47 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS) includes measures on the reliability and security of critical network and information systems, including incident reporting

requirements. NIS came into force in August 2016 and is to be implemented by Member States by May 2018.

8.48 Under NIS, operators of essential services are required to provide notification to their competent authority in the event "of incidents having a significant impact on the continuity of essential services they provide".

8.49 Credit institutions are defined as operators of essential services under NIS, in so far as they meet the criteria set out in Article 5(2). The EBA's guidelines on Major Incident Reporting confirm that the requirements for notification of incidents under PSD2 are considered to be at least equivalent to the obligations in NIS. Therefore incidents affecting credit institution's payment services should be reported under PSD2 rather than NIS.

The Interchange Fee Regulation (IFR)

8.50 The IFR is a directly applicable EU regulation[12], which introduced obligations for PSPs dealing in card-based payments which are complementary to the requirements under PSD2. We are jointly competent with the Payment Systems Regulator for some of these provisions. The majority of IFR rules relating to business obligations for PSPs conducting business in card-based payments took effect on 9 June 2016.

8.51 The Payment Systems Regulator has produced guidance setting out its approach in relation to its functions under the IFR.

Data protection legislation

8.52 PSPs need to be aware of their obligations under the Data Protection Act 1998, as well as the upcoming changes to the data protection regime under the General Data Protection Regulation ((EU) 2016/679) which comes into effect on 25 May 2018.

8.53 There are a number of areas in the PSRs 2017 where a PSP's obligations will interact with their obligations under the data protection regime.

8.54 Where possible, we have included guidance on how the requirements under the PSRs 2017 interact with data protection legislation throughout this chapter.

Anti-money laundering and terrorist financing legislation

8.55 All PSPs and e-money issuers must comply with the Money Laundering and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs) to counter the risk that they are misused for the purposes for money laundering and terrorist financing. The obligations include identifying customers, monitoring transactions and identifying and reporting suspicious transactions.

8.56 EU Regulation 2015/847 on information accompanying transfers of funds (Funds Transfer Regulation) is a directly applicable EU regulation that specifies the information on the payee or payer to be included in a payment message (or made

[12] Regulation (eu) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R0751&from=en

available on request) and the circumstances that a PSP is required to verify that information.

- For businesses supervised by the FCA under the MLRs, the Joint Money Laundering Steering Group has provided guidance on interpreting these obligations and the FCA has a financial crime guide.
- For businesses supervised by HMRC under the MLRs (for example those only undertaking the payment service of money transmission) they have provided *guidance on complying with AML and CFT obligations*.
- **Chapter 19 - Financial Crime** contains further details about these requirements.

Part I: Information requirements

8.57 The information that PSPs are required by the PSRs 2017 to provide to customers is separated into two scenarios:

- Transactions under framework contracts – a contract governing the future execution of individual and successive payment transactions (see regulation 2 for the full definition). This is where there is an ongoing relationship, and there is an agreement between the PSP and the customer covering the making of payments. Examples of this would be parts of a bank's current account terms and conditions or a PI or EMI's contract with its customer.
- Single payment transactions – this is typically where there is no ongoing relationship between the customer and the PSP – the transaction is a "one-off" and the contract between the PSP and the customer relates solely to the particular transaction in question. A single payment transaction may also occur if there is a framework contract that does not include the particular payment service involved.

8.58 For both scenarios, the PSRs 2017 set out the information to be provided before the contract is entered into, before execution of the transaction, and after execution of the transaction.

8.59 As set out at paragraph 8.18, where a PSP provides a payment service and grants credit, the general principle is that the two regulatory regimes apply cumulatively. However, there are some exceptions to this. Regulation 41 of the PSRs 2017 sets out the interaction between the PSRs 2017 and the consumer credit regime in relation to Part 6 of the PSRs 2017.

8.60 Regulation 41(2) provides that:

- regulation 50 (changes in contractual information) does not apply
- regulation 51 (termination of framework contract) does not apply

8.61 We have summarised the requirements of regulation 41(2) of the PSRs 2017 and how, in our view, it applies to any credit cards and overdrafts which are regulated by the CCA below. This table does not set out other legal requirements which may apply (for example under CONC or the Consumer Rights Act 2015).

	Current account with an overdraft regulated by the CCA	Credit card regulated by the CCA
Regulation of the PSRs 2017	**Do the PSRs 2017 apply?**	
Regulation 50 - changes in contractual information	Regulation 50 will **not** apply to making changes to the terms of the overdraft (including debit interest rates). Changes to these will be governed by applicable provisions in the CCA. Regulation 50 will apply to any changes to the framework contract for payment services (including credit interest rates).	Regulation 50 will **not** apply. Changes to contractual information (including debit interest rates) will be governed by applicable provisions in the CCA.
Regulation 51 - termination of framework contract	[Subject to HMT consultation question]	Regulation 51 will **not** apply. Termination will be governed by applicable provisions in the CCA.

8.62 Regulation 41(3) also provides that, where a PSP is required to provide the same information to a customer under the PSRs 2017 and the consumer credit regime, information which has been provided in compliance with the consumer credit regime does not need to be provided again in order to comply with the PSRs 2017.

8.63 However, the requirements of the PSRs 2017 and the consumer credit regime apply cumulatively, so this is only the case if the information was provided in a manner which complies with the requirements of the PSRs 2017. This means that information does not need to be duplicated unnecessarily, but PSPs still need to be satisfied that they are meeting the information requirements under both the PSRs 2017 and consumer credit regime. For example, any pre-contractual information provided in a SECCI for a credit card would not need to be duplicated to meet requirements under regulation 48 of the PSRs 2017, but any information **not** included in the SECCI would still need to be provided to the customer in accordance with regulation 48 of the PSRs 2017.

Form in which the information must be provided (regulation 55)

8.64 The information must be provided or made available:

- in easily understandable language and in a clear and comprehensible form
- in English (or other agreed language)
- in the case of single payment contracts, in an easily accessible manner
- on paper or another durable medium (for single payment contracts, only where the customer requests this) unless otherwise specified in the particular regulation or in some cases, subject to agreement.

8.65 A distinction is drawn in the regulations between "making available" information and "providing" it. In line with the recitals to PSD2 and Court of Justice of the European Union ("CJEU") case law, we expect information which is required to be "provided" to be actively communicated by the PSP to the customer without any prompting by the customer.

8.66 In contrast, a requirement to make information available means that the customer can be required to take active steps to obtain the information (for example, by requesting it from the PSP, logging on to a messaging system within online banking or inserting a bank card into a printer for account statements), but access must be possible and the information must be readily available.

8.67 So for example, a PSP would only be making information available if they upload it to the customer's electronic inbox in the provider's own online banking website. However, if they send an email to the address regularly used by the customer to communicate with other people or an SMS notification to the customer's phone in accordance with an agreement in the framework contract to say that a document has been uploaded to a customer's online banking account, this could be sufficient to meet a requirement to provide the information.

8.68 We expect providers to adopt an approach to the information requirements that takes account of the confidentiality of the information concerned and any particular needs of the customer.

8.69 Durable medium is defined as "any instrument which enables the payment service user to store information addressed personally to them in a way accessible for future reference for a period of time adequate for the purposes of the information and which allows the unchanged reproduction of the information stored". As set out in recital 57 this may be met by printouts on account printers, CD-ROMs, DVDs, the hard drives of computers on which emails can be stored, and, in certain circumstances internet sites. However, we acknowledge that many forms of media are capable of meeting the criteria of being a durable medium.[13]

8.70 This definition has been considered recently by the CJEU in the context of internet sites. In line with the court's findings we consider that, to be a durable medium, a website or an instrument must be functionally equivalent to paper. In particular it must:

- give customers control of the information
- allow storage for long enough to enable them to enforce their rights
- exclude the possibility of the PSP or person acting for them changing the content

8.71 Putting information on a PSP's 'ordinary' website would not meet durable medium requirements if the PSP has full control of the information and the ability to change or delete it.

[13] https://www.fca.org.uk/firms/durable-medium [also see CP17/7 Insurance Distribution Directive implementation – consultation paper I]

8.72 No charges may be levied by the PSP for providing any of this information, in the form and frequency required by the PSRs 2017.

8.73 A FSMA authorised firm which is also carrying on an activity regulated under FSMA will need to take into account the Communications with Clients Principle, which requires it to communicate information to clients in a way that is clear, fair and not misleading. All PSPs also need to be aware of their obligations under the Consumer Protection from Unfair Trading Regulations 2008 and the Consumer Rights Act/UTCCRs (as applicable).

8.74 In our view, the requirements to deliver information in a certain way in Parts 6 and 7 of the PSRs 2017 can be summarised as follows (subject to any specific requirements in a particular regulation):

Requirement	**Meaning of requirement**
"Provide"	Needs to be actively communicated to the customer without any prompting by the customer. Examples are SMS, email or letter sent to customer.
"Make available"	Customer can be required to take active steps to obtain the information. An example is uploading information to a customer's online banking account for them to access.

A. Framework contract
Before the framework contract is entered into (regulation 48 and Schedule 4)

8.75 In good time before the contract is concluded (or immediately after the execution of the transaction if the contract has been concluded at the customer's request by means of distance communication, such as by telephone, where it is not practicable to make the information available beforehand), the PSP must provide the customer the information in the table below.

8.76 This can be done by providing the customer with a copy of the draft contract. For distance contracts concluded online, we expect PSPs to be able to provide information beforehand. PSPs could achieve this by, for example, emailing the customer the terms of the framework contract and Schedule 4 information as part of the process.

Information to be provided before the contract is entered into (regulation 48 and Schedule 4)

Details about the PSP	The PSP's name, head office address and contact details. If different, the address and contact details of the branch or agent from which the service is being provided and details of the PSP's regulator(s), including any reference or registration number (for example the provider's Financial Services Register number).
Details of the payment service(s) to be provided	Description of the main characteristics.
	Specification of the information or unique identifier to be provided by the customer for a payment order to be properly initiated or executed. For example, for a UK bank transfer, the payee bank's sort code and account number might be specified as the unique identifier. The importance of providing the correct unique identifier (and the potential for loss/delay if an incorrect unique identifier is provided) should be explained to the customer.
	What the PSP will take as consent for the initiation of a payment order or the execution of a payment transaction, and the procedure by which such consent may be given. For example, consent could be given in writing, verified by a signature, by means of a payment card and PIN number, over a secure password-protected website, by telephone or by use of a password. Whatever means are to be used, including any allowable alternative methods (eg signature in place of chip and PIN), must be detailed in the framework contract. The contract must also set out the procedure by which the customer may withdraw consent. These processes must be in line with the requirements of regulation 67 (consent and withdrawal of consent) and 100 (authentication).
	Details of when a payment order will be deemed to have been received in accordance with regulation 81 (including details of deemed receipt for future dated and recurring transactions). If the PSP has a cut-off time near the end of the business day after which payment orders are deemed to have been received on the next business day, this must be specified. This is very important because of the requirements in the PSRs 2017 on execution time of payments. It is recognised that there may be different cut-off times for different payment channels.

	The maximum time after receipt of a payment order, by which the funds will have been credited to the payee's PSP's account. This must be in line with the requirements of regulation 86.
	Where applicable, the fact that a spending limit may be agreed for a payment instrument attached to the account (for example, a maximum daily withdrawal limit on an ATM card), although the spending limit itself (eg £250) does not form part of the Schedule 4 information. To avoid doubt, a spending limit differs from a credit limit.
	In relation to co-badged card-based payment instruments, details of the customer's rights under Article 8 of the Interchange Fee Regulation (EU 2015/751). This means PSPs need to provide details of the customer's right to require two or more different payment brands on a card-based payment instrument (provided that such a service is offered by the PSP).
Charges and interest	Details of all charges payable by the customer to the PSP and, where applicable, a breakdown of them. The customer should be able to understand what the payment services to be provided under the contract will cost them. We take "where applicable" in this context to mean that, where charges are capable of being broken down into constituent parts to provide more transparency to customers, they should be broken down. A PSP only needs to provide details of the amount that it will charge the customer (ie where a payment is initiated through a PISP, details of the amounts charged by that PISP do not need to be provided by the ASPSP). Where accounts are in scope of the Payment Account Regulations 2015, PSPs will need to consider their obligations to provide a fee information document in addition to their requirements under the PSRs 2017. If the PSP will make a charge for notifying the customer that a payment order has been refused under regulation 82, this must be specified here. If the PSP will make a charge for providing or making information available in accordance with regulation 56(2) (eg a charge for additional or more frequent information or information transmitted in a different manner), this must be specified here as well.

	Details of the interest or exchange rates to be used (where relevant). This will include changes to interest rates on the underlying payment account unless the use of reference rates has been agreed (as set out below). If a reference exchange or interest rate is to be used, details of where the reference rate can be found and how the actual rate will be calculated must be given (including the relevant date and index or base for determining the reference rate). The aim is to enable the customer to verify that the interest charged or paid is correct or that the exchange rate applied to a transaction is correct. In practice, this means that a PSP would need to include details of when it will actually apply the rate to the account or transaction (eg for exchange rates with an externally set reference rate and margin, the PSP will need to provide details of when it actually converts the monies so that the customer can look at the appropriate date on the website for the externally set rate to verify whether the amount charged is correct). Reference exchange rates may be set by the PSP itself, but the customer must be told where they can find out what they are. Reference interest rates cannot be set by the PSP and need to be publicly available.
	Agreement, if relevant, that changes in reference interest or exchange rates will take effect immediately (otherwise they will take effect in line with regulation 50(1)).
	Where reference interest or exchange rates are being used, agreement, of how, and with what frequency changes in actual interest or exchange rates will be notified, in line with regulation 50(5). If no alternative method or frequency is agreed, notification will be required as soon as possible.
Transmission of information	How information relating to the account will be transmitted (for example, in writing, to an agreed email address or using a secure website), how often it will be provided or made available and what language will be used. Any technical requirements for the customer's equipment and software to receive information or notices must be stated. The contract must also include the customer's right to obtain a copy of the contract at any time during its term.
Information about safeguards and corrective measures	What steps the customer must take to keep a payment instrument safe. (Note that 'payment instrument' has a wide definition and will include payment cards, e-banking and telephone banking arrangements.)
	Details of how to notify the PSP of the loss, theft or misappropriation of the payment instrument.
	Details of the secure procedure which the PSP will follow to contact the customer in the event of suspected or actual fraud or security threats.

	In what circumstances the PSP would be able to stop or block the payment instrument. These are limited to reasons related to: • the security of the payment instrument; • the suspected unauthorised or fraudulent use of the payment instrument • where the payment instrument has a credit line (for example, a credit limit on a credit card), a significantly increased risk that the payer may be unable to pay it back PSPs may wish to include wording advising that the payment instrument might be blocked or stopped due to national or Union legal obligations of the PSP.
	In what circumstances and to what extent the customer might be liable for unauthorised payment transactions.
	That the customer must notify the PSP of any unauthorised or incorrectly initiated or executed payment transactions as soon as they become aware of them, how such notification should be made and that the notification should be no later than 13 months after the debit date in order to be entitled to have the error corrected (no such limit will apply unless the customer has received this information). It is open to the PSP to offer better terms in this area.
	The PSP's liability for unauthorised or incorrectly initiated or executed payment transactions (for example that the PSP will be liable for unauthorised or incorrectly initiated or executed payment transactions, as long as the claim is made within the time limits specified above). If UK Direct Debits are offered as a payment service on the account, reference should be made to the rights under the Direct Debit Guarantee scheme.
	The conditions under which a refund is payable in relation to a transaction initiated by or through a payee (for example, a direct debit or card transaction).
Information about the length of the contract, variation of terms and termination	The duration of the contract, customer and PSP termination rights, and the terms under which it can unilaterally vary the contract.
Information on applicable law and disputes	Details of the law applicable to the contract, the competent courts, the availability of the FOS or (for users that would not be eligible to complain to FOS) another dispute resolution service, any other alternative dispute resolution procedures available to the customer (for example, under the Online Dispute Resolution Regulations (EU 524/2013), how to access them (see **Chapter 11 - Complaint handling**) and the possibility to submit complaints to us.

Information during period of contract (regulation 49)

8.77 The customer is entitled to request the information specified in Schedule 4 and the terms of the framework contract at any time during the course of its contract with a PSP. If the customer requests this, it must be provided to the customer (sent or given directly to the customer) on paper or another durable medium free of charge.

Changes to the framework contract (regulation 50)

8.78 For most changes to the framework contract, or to the information that has to be disclosed before the framework contract is entered into (ie the information detailed in paragraph 8.40), PSPs must provide any proposed changes at least two months before they are due to take effect. This principle applies irrespective of whether the changes are favourable or unfavourable to the customer (although see below for changes to interest or exchange rates). PSPs will also need to ensure that their variation terms and their proposed variations comply with the CRA or UTCCRs as applicable.

8.79 Some account terms and conditions will contain provisions relating to other, non-payment services, for example terms and conditions relating to cheques. In such cases the obligation to notify changes under regulation 50 does not extend to non-payment services that are outside the scope of the pre-contract disclosure requirement. However, for banks and building societies the BCOBS requirements on appropriate information and making changes may apply to such services.

8.80 The framework contract may contain a provision that changes are to be made unilaterally unless the customer notifies the PSP to the contrary (although PSPs will also need to take account of unfair contract terms legislation when including such a provision). It may also state that rejection of proposed changes will amount to rejection of the contract and notice of termination. If the contract contains such a provision, the advice of change must state:

- that the customer will be deemed to have accepted the changes unless they notify the PSP before the proposed date of the change
- that the customer has the right to terminate the contract immediately and without charge before that date

8.81 The addition of new payment services to an existing framework contract, which do not change the terms and conditions relating to the existing payment services, will not be treated as a change and so will not require two months' notice under regulation 50 of the PSRs 2017, though other legislation such as the CRA/UTCCRs will still apply.

8.82 In general, we believe a change in account type at the PSP's instigation - e.g. from a 'free account' to a fee paying packaged account - constitutes either a change in the framework contract or a termination of the existing contract and its replacement by a new framework contract. Both the proposed change and the termination by the PSP require the customer to be given two months' notice, and the option of immediate termination without charge.

8.83 The exception to the two month rule is making changes to interest and exchange rates. These may be applied immediately and without prior notice if:

- changes to the actual interest or exchange rates arise from changes to a reference interest rate or a reference exchange rate (assuming this has been agreed in the framework contract and the information specified in Schedule 4 to the PSRs 2017 in respect of the reference interest or exchange rate has been properly disclosed)
- where the changes are more favourable to the customer

8.84 In both cases, the customer must be notified of the changes as soon as possible unless another specific frequency has been agreed. In all cases, PSPs should make it clear to the customer when the changes to the actual rates (which track the changes to the reference rate) will be applied. For example, immediately or the business day after the change in the reference rate. The manner in which this information is to be provided or made available must be agreed with the customer.

8.85 The application of interest rate or exchange rate changes must be implemented and calculated in a neutral manner that does not discriminate against customers. In our view, this means that customers should not be unfairly disadvantaged; for example, by using a calculation method that delays passing on changes in rates that favour customers but more quickly passes on changes in the PSP's favour.

8.86 Recital 54 of PSD2 makes clear that the intent of the information provisions in the directive, and therefore in the regulations, is to enable payment service users to make well-informed choices, and to enable consumers to shop around within the EU. In light of this, and the stipulation in regulation 50(1)(a) that changes in the specified information in Schedule 4 also require pre-notification, we would expect that where, for example, an introductory interest rate on a payment account comes to an end, PSPs should provide notice of the change in the interest rate, as specified in the table below paragraph 8.76.

8.87 Relying on a framework contract term stating that the interest rate will change at the end of the introductory period, is not, in our view, sufficient. However, the notification requirement does not necessarily extend to all other interest rate changes agreed in the framework contract. For example, where an account has a tiered interest rate structure, under which higher balances attract higher rates, changes within that structure due to changes in the underlying balance would not require pre-notification. Similarly, it would not be necessary to give pre-notification of the end of a bonus rate if it was clear from the customer information provided at the outset that the bonus rate lasted less than two months.

8.88 Where the contract relates to a payment service in relation to funds covered by a credit line provided under a regulated agreement under the CCA, regulation 50 does not apply. See paragraph 8.61 for further details.

8.89 We would expect that, in normal circumstances, where a change in UK or EU legislation or regulation requires a change to be made in the framework contract, businesses will be sufficiently aware of forthcoming changes in legislation or regulation and therefore able to provide the required two months' notice set out above. However, it is recognised that there may be exceptional occasions where this may not be possible.

Where this is the case, customers should be given as much notice of the changes as possible.

Termination of the framework contract (regulation 51)

8.90 The framework contract may be terminated by the customer at any time, unless a period of notice (not exceeding one month) has been agreed. If the contract has been running for 6 months or more, no charge may be made for termination. Regular service charges for the running of the payment services may be charged, but any advance payments in respect of such service charges must be returned on a pro-rata basis. Any charge that is made for termination must reasonably correspond to the PSP's actual costs.

8.91 If agreed in the framework contract (and subject to the UTCCRs/CRA), the PSP may terminate a framework contract that is not for a defined term by giving at least two months' notice of termination to the customer.

8.92 The parties retain their usual legal rights to treat the framework as unenforceable, void or discharged, in line with usual contract law principles.

8.93 Where the contract relates to a payment service in relation to funds covered by a credit line provided under a regulated agreement under the CCA, regulation 51 does not apply. See paragraph 8.61 for further details.

Transaction information under a framework contract

Before execution (regulation 52)

8.94 Where the payment order is given direct by the payer customer to his PSP, the PSP must, at the customer's request, inform the customer of:

- the maximum execution time for the transaction concerned
- any charges payable (including a breakdown of those charges where applicable)

After execution (regulations 53 and 54) **[version 1: guidance based on Treasury exercising the member state option]**

8.95 **[Version 1 starts:]** Under regulations [53 and 54] the PSP must provide its customer with certain information on transactions.

8.96 This information must be provided on paper or on another durable medium at least once a month, free of charge. As we have described at paragraph 8.77, as the information needs to be provided this means it must be sent or given to the customer. We have set out in paragraph 8.69 our understanding of the meaning of durable medium.

8.97 It is important to note that these provisions do not require monthly statements to be provided for all accounts. Where there are no transactions (or the only transactions relate to the payment of interest) there is no obligation under the PSRs 2017 to provide the information (although, where relevant, PSPs will need to satisfy themselves that they are complying with the requirement to provide statements under s78(4) CCA). **[Version 1 ends:]**

After execution (regulations 53 and 54) **[version 2: guidance based on Treasury not exercising the member state option]**

8.98 **[Version 2 starts:]** As soon as reasonably practicable after each individual transaction, the PSP must provide its customer with certain information.

8.99 Where a PSP's customer is the payer, the PSP must include a condition in its framework contract which gives the customer the option to require the information to be provided or made available free of charge at least once a month. The way that the information will be provided or made available must be agreed with the customer and it must be in a form which allows it to be stored and reproduced unchanged. If the customer does not exercise this option the information must be provided on a transaction by transaction basis, as soon as reasonably practicable, in line with regulation 53(1).

8.100 Where a PSP's customer is the payee, a PSP may provide in its framework contract that the information will be provided or made available at least once a month. The way that information will be provided or made available must be agreed with the customer and it must be in a form which allows it to be stored and reproduced.

8.101 As we have described at paragraph 8.77, where information needs to be provided this means sent or given to the customer. Where information only needs to be made available, this means available to obtain at the customer's option.

8.102 Subject to the inclusion of suitable terms and conditions in the framework contract and the customer exercising the option provided for in the framework contract, the requirements of regulations 53 and 54 can be met by means of issuing (or making available) a monthly statement. This can be through a secure website that meets the requirements for being a durable medium, or on request (although it must be made clear to the customer that the information is being made available and how to obtain it). For accounts operated by use of a passbook, our view is that the transaction information is available to customers when they present their passbooks to be made up and that this is sufficient to fulfil the obligation to "make available".

8.103 It is important to note that these provisions do not require monthly statements to be provided for all accounts. Where there are no transactions (or the only transactions relate to the payment of interest) there is no obligation under the PSRs 2017 to provide the information (although, where relevant, PSPs will need to satisfy themselves that they are complying with the requirement to provide statements under s78(4) CCA). **[Version 2 ends:]**

8.104 This is the information required for the payer:

- a reference enabling the customer to identify the payment transaction and, where appropriate, information relating to the payee. This information should assist the customer in helping to check that a payment has not been misdirected.
- the amount of the transaction in the currency of the payment order, along with details of any exchange rate used by the PSP and the amount of the payment transaction after it was applied
- the amount and, where applicable, breakdown of any transaction charges and interest payable in respect of the transaction, so that the customer knows the

total charge to be paid. We would also expect the breakdown provided by PSPs under this regulation to correspond with the breakdown provided pre-contractually, so that customers are able to verify that the charges applied to a transaction are correct. The PSRs 2017 allow the inclusion of a reference exchange rate in framework contracts where the actual exchange rate used in a transaction is based on that published rate plus a margin also set out in the framework contract. While there is no requirement in the PSRs 2017 for this margin to be separately listed in the transaction information there is a requirement that any fees be listed. Therefore, where adjustments to the reference exchange rate are expressed in the framework contract as a fee, the amount of this fee should be disclosed separately

- where applicable, the exchange rate used by the payer's PSP and the amount of the payment transaction after that currency conversion
- the debit value date or date of receipt of the payment order

8.105 This is the information required for the payee:

- a reference enabling the customer to identify the payment transaction and the payer and any information transferred with the payment transaction. The Funds Transfer Regulations require, for anti-money laundering and counter-terrorist-financing purposes, certain details of the payer and the payee to be transferred with such payments (or in some cases to be available to the payee's PSP on request)
- the amount of the transaction in the currency of the payment account credited
- the amount and, where applicable, breakdown of any transaction charges and/or interest payable in respect of the transaction. We would also expect the breakdown provided by PSPs under this regulation to correspond with the breakdown provided pre-contractually, so that customers are able to verify that the charges applied to the transaction are correct
- any exchange rate used by the payee's PSP and the amount of the payment transaction before it was applied the credit value date

Low value payment instruments (regulation 42)

8.106 Low value payment instruments are those that under the framework contract:

- can only be used for individual transactions of €30 (or equivalent) or less, or for transactions executed wholly within the UK €60 (or equivalent) or less
- have a spending limit of €150 (or equivalent), or for payment instruments where payment transactions can only be executed within the UK, €300 (or equivalent)
- store funds that do not exceed €500 (or equivalent) at any time

8.107 The following, less detailed, information requirements apply to low value payment instruments, relating to information required before entering into a framework contract (or immediately after the execution of the transaction if the contract has been concluded by some means of distance communication (for example, by telephone) where it is not practicable to do so) and information required before individual payment transactions.

8.108 The PSP must provide information on the main characteristics of the payment service.

8.109 This must include:

- the way in which the instrument can be used
- the payer's liability for unauthorised payment transactions
- details of any charges applicable
- any other material information that the customer might need to make an informed decision
- details of where the customer can easily access the full information in Schedule 4 that must normally be disclosed prior to being bound by a framework contract (as specified in Schedule 4 (for example, the website URL))

8.110 It may also be agreed that rather than full post-execution information on payment transactions the PSP may provide or make available a reference that will enable the customer to identify the individual transaction, the amount and any charges payable in respect of the transaction. If there are several payment transactions of the same kind to the same payee, the PSP must provide or make available information on the total amount of the transactions concerned and any charges for those payment transactions.

8.111 If the payment instrument concerned is used anonymously or, for technical reasons the PSP is not able to provide or make available even this limited post-execution information, it does not need to be provided. However, the PSP must enable the customer to check the amount of funds stored.

8.112 The PSP and the customer may also agree that changes to the framework contract relating to the low value payment instrument do not have to be communicated in the form and manner required for other framework contract changes (ie they can agree that there is no need to communicate the changes on paper or another durable medium).

8.113 We recognise that fluctuations in exchange rates between euro and sterling may cause difficulties over time in determining whether a particular payment instrument is a low value payment instrument. We expect PSPs to take a reasonable and consistent approach to dealing with such fluctuations to ensure they are compliant with the requirements.

B. Single payment transactions

Before the transaction (regulation 43 and Schedule 4)

8.114 Before the contract is concluded (or immediately after the execution of the transaction if the contract has been concluded by some means of distance communication (for example, by telephone) where it is not practicable to do so), the PSP must provide or make available to the customer the information set out below in relation to the service. This may be done, for example, by providing the customer with a copy of the draft contract or payment order:

- the information (or unique identifier) the customer needs to provide for the payment order to be properly initiated or executed (the payment routing information)

- the maximum time the payment service will take to be executed (that is, how long until the funds are received). This must be in line with the requirements of regulation 86
- details of any charges, including a breakdown where applicable
- if applicable the exchange rate to be used (or the reference exchange rate on which the actual exchange rate will be based)

8.115 In addition, there is a list of information in Schedule 4 of the PSRs 2017 that must be disclosed prior to entering into a framework contract. Items on the list must also be provided or made available if they are relevant to the single payment contract in question. What is "relevant" will depend on the nature of the payment service and the circumstances. However, we consider that the following, in particular, will always be relevant information:

- details of the PSP and its regulators (Schedule 4, paragraph (1))
- a description of the main characteristics of the payment service to be provided (Schedule 4, paragraph (2)(a)). Due to the nature of the service provided by PISPs, we would expect a description of the service to include, as a minimum, details of (i) how the payment initiation service works alongside the customer's account and (ii) how the PISP accesses the customer's account with the ASPSP. The information should be presented in a way which is easy for customers to understand.
- any contractual clause on governing law and jurisdiction (Schedule 4, paragraph (7)(a))
- for customers who are eligible to take complaints to the FOS, notification of the availability of the FOS or (for users that would not be eligible to complain to FOS) another dispute resolution service, any other alternative dispute resolution procedures available to the customer (for example, under the Online Dispute Resolution Regulations (EU 524/2013) and how to access them (Schedule 4, paragraph (7)(b))

8.116 Where a PI operates as a wholesaler (providing a payment service to smaller money transfer operators but without having a contractual relationship with the payment service user) and provides its client PIs with advertising materials and stationery, they must make it clear to customers of client before any transaction is entered into, that the client is the PSP. A failure to do so is likely to constitute a breach of the PSRs 2017.

8.117 Advertising and marketing material or business stationery that is likely to mislead the customer into believing the PSP with whom they are contracting is the wholesaler rather than the client, may also potentially constitute an unfair commercial practice under the CPRs. Where it appears to us that a PSP's business model has been changed from an agency to a wholesaler model purely as a matter of form rather than substance to avoid its regulatory obligations for its agents, this would be seen as a matter of concern.

8.118 Before a payment is initiated, in addition to the above information, PISPs must provide or make available to the payer clear and comprehensive information covering:

- the name and head office address of the PISP

- if the PISP uses an agent or branch to provide services in the UK, the address of that agent or branch
- any other contact details to be used to communicate with the PISP including an email address
- our contact details

After the initiation of a payment order (regulation 44)

8.119 A PISP has to provide or make available to the payer the information below immediately after the payment order is initiated and, where applicable, to the payee.

8.120 The information is as follows:

- confirmation that the payment order has been successfully initiated with the payer's ASPSP
- a reference enabling the payer and the payee to identify the payment transaction and, where appropriate, the payee to identify the payer, and any information transferred with the payment order
- the amount of the payment transaction
- the amount of any charges payable to the PISP in relation to the payment transaction and, where applicable, a breakdown of the charges

8.121 The PISP must also provide or make available the reference for the payment transaction to the customer's ASPSP. This is likely to be the same reference as provided to the payer and payee under regulation 44(1)(b).

After the receipt of the payment order (regulation 45)

8.122 The payer's PSP must immediately after receipt of the payment order, provide or make available to his customer the following information in relation to the service it is providing:

- a reference to enable the payer to identify the transaction (and if appropriate the information relating to the payee, for example, in a money remittance what the payee will need to do to collect the funds)
- the amount of the payment transaction in the currency used in the payment order
- details of any charges (including, where applicable, a breakdown of those charges)
- where the transaction involves a currency exchange and the rate used differs from the rate provided before the transaction, the actual exchange rate used (or a reference to it) and the amount of the payment after the currency conversion. In practice, this means that PSPs need to know the actual exchange rate that will be used at this point so that they can provide or make this information available to customers. In our view, providing or making an indicative rate available to customers at this stage would not be sufficient.
- the date the payment order was received

Information for the payee after execution (regulation 46)

8.123 The payee's PSP must immediately after execution of the payment transaction provide or make available the following to the customer in relation to the service it is providing:

- a reference to enable the payee to identify the transaction and where appropriate, relevant information transferred with it (for example, name of the payer and invoice number). The Funds Transfer Regulations require, for anti-money laundering and counter-terrorist-financing purposes, certain details of the payer and the payee to be transferred with such payments (or in some cases to be available to the payee's PSP on request).
- the amount of the transaction in the currency in which the funds are being put at the payee's disposal
- details of any charges (including, where applicable, a breakdown of those charges)
- the exchange rate used (if relevant) and the amount of the payment before it was applied
- the credit value date

Avoidance of duplication of information (regulation 47)

8.124 If the single payment transaction arises from the use of a payment instrument issued under a framework contract with one PSP, the PSP with whom the single payment transaction is undertaken need not provide information that will be provided or made available by the former PSP under the framework contract.

C: Other information provisions

Charges for information (regulation 56)

8.125 The information specified above must be provided free of charge. PSPs may charge for the additional or more frequent provision of information requested by the customer, or where another means of transmission from that agreed in the framework contract is requested by the customer, but these charges must reasonably correspond to the actual cost to the PSP of providing the information. PSPs must therefore be able to justify the level of any charges.

Currency conversions (regulation 57)

8.126 Payment transactions must be executed in the agreed currency. Where a currency conversion service is offered before a payment transaction, at an ATM, at the point of sale or by the payee (that is, "dynamic currency conversion" where, for example, a UK shop could offer German customers the facility to pay their bill in euro) the exchange rate to be used and all charges must be disclosed to the customer before the transaction is agreed. It is the person offering the service who must comply with the disclosure obligation – if that person is not a PSP then failure to make the disclosure risks committing a criminal offence under regulation 141.

Information on additional charges or reductions (regulation 58)

8.127 If a payee (typically a shop, website operator or other merchant) levies an additional charge or offers a reduction in cost for using a particular means of payment (for example an additional charge for using a credit card) this information must be advised to the customer before the start of the payment transaction.

8.128 Similarly, if a PSP or any other party involved in a transaction charges for the use of particular payment instrument, it must inform the customer of such charges before the payment transaction is initiated. A third party that fails to do so risks committing a criminal offence under regulation 141 and may also be in breach of the Consumer Protection from Unfair Trading Regulations.

8.129 The customer is not obliged to pay the charges if they have not been informed of the full amount of the charges in accordance with the requirements of regulation 58.

8.130 Where payees are levying additional charges, they need to be aware of their obligations under other legislation, eg the Consumer Rights (Payment Surcharges) Regulations 2012.

Burden of proof (regulation 59)

8.131 The burden of proof is on the PSP to show that it has met the information requirements in Part 6. PSPs will need to ensure that they keep appropriate records to demonstrate the provision of information to customers in the appropriate way. This provision also applies to RAISPs

Information requirements for RAISPs (regulation 60)

8.132 RAISPs do not have to provide as much information to their customers as other PSPs.

8.133 RAISPs must always provide details of the information or unique identifier to be provided by the customer in order to use the service (eg user name, password, etc) and all charges payable by the customer to the RAISP and, where applicable, a breakdown of those charges.

8.134 RAISPs must also provide any information specified in Schedule 4 which is relevant to the service provided. What is 'relevant' will depend on the nature of the service and the circumstances. However, we consider that the following, in particular, will always be relevant information:

- the name, address and contact details of the RAISP's head office
- details of the RAISP's regulators, including the RAISP's registration number
- A description of the main characteristics of the service. Due to the nature of the service provided by RAISPs, we would expect a description of the service to include, as a minimum, details of (i) how the account information service works alongside the customer's account and (ii) how the AISP accesses the customer's account with the ASPSP. This should be presented in a way which is easy for customers to understand.
- any contractual clause on the law applicable to the framework contract and the competent courts

8.135 The burden of proof is on the RAISP to show that it has met the relevant information requirements (see the table below paragraph 8.76 for the relevant information requirements).

8.136 RAISPs also need to be aware of any obligations under data protection law which apply to them, including requirements to be transparent about how data will be used and to give customers appropriate privacy notices when collecting personal data.

Part II: Rights and obligations in relation to the provision of payment services

8.137 The COB provisions on rights and obligations contain rules on:

- charging
- authorisation of payment transactions
- access to payment accounts for AISPs and PISPs
- execution of payment transactions
- execution time and value date
- liability

General (regulations 63-65)

8.138 These provisions apply to payment transactions under framework contracts and single payment transactions. They apply to low value payment instruments unless otherwise stated. See Part I, Section A of this chapter for a definition of low value payment instruments.

8.139 These provisions also apply to payment services provided in relation to funds covered by a credit line provided under a regulated agreement for the purpose of the CCA, but certain provisions are disapplied.

8.140 Regulation 64 of the PSRs 2017 set out the interaction between the PSRs 2017 and the consumer credit regime in relation to Part 7 of the PSRs 2017. It provides that:

- regulations 71(2)–71(5) (limits on the use of payment instruments) do not apply where section 98A(4) of the CCA applies
- regulations 74, 76 and 77 (rectification of liability for unauthorised transactions) do not apply

8.141 We have summarised the requirements of regulation 64 of the PSRs 2017 and how, in our view, it applies to any credit cards and overdrafts which are regulated by the CCA below. This table does not set out other legal requirements which may apply (for example under CONC or the Consumer Rights Act 2015).

	Current account with an overdraft regulated by the CCA	**Credit card regulated by the CCA**
Regulation of the PSRs 2017	**Do the PSRs 2017 apply?**	
(1) Regulation 71(2) to (5) - limits on the use of payment instruments	Regulations 71(2) to (5) of the PSRs 2017 apply to overdrafts. This is because Regulations 71(2) to (5) are only disapplied where s98A(4) of the CCA applies. Section 98A(4) of the CCA does not apply to overdrafts.	Regulations 71(2) to (5) do not apply to credit cards. Section 98A(4) of the CCA applies.

	(2) Regulations 74, 76 and 77 - rectification of and liability for unauthorised transactions	For current accounts with overdrafts, the PSRs 2017 regime will apply in relation to transactions or parts of transactions which occur when the customer is in a credit position and the CCA in relation to transactions or parts of transactions which occur when the customer is in a debit position. Where an unauthorised transaction takes an account from a credit position to an overdrawn position, both regimes will apply (i.e. the PSRs 2017 will apply to the amount that was taken from the credit position and the consumer credit regime will apply to the amount that was taken from the overdraft).	For credit cards, regulations 74, 76 and 77 will not apply and the equivalent regime in the CCA will apply.

Requirements for RAISPs (regulation 63(4))

8.142 The following regulations apply to RAISPs:

- regulation 70 (access to payment accounts for account information services)
- regulation 71(7)-71(10) (denial of access to an AISP)
- regulation 72(3) (obligations on payment service user in relation to payment instruments and personalised security credentials)
- regulation 99 (incident reporting)
- regulation 100 (authentication)

RAISPs do not need to comply with any other provisions in Part 7 of the PSRs 2017.

Charges (regulation 66)

8.143 PSPs may only charge their customers for carrying out their obligations as set out in Part 7 of the PSRs 2017 (those concerning rights and obligations) where the PSRs 2017 specifically allow it. Those charges must be agreed with the customer and must reasonably correspond to a provider's actual costs. The corporate opt-out applies to this provision (see under "General" at the start of Part II).

8.144 Where the payer's PSP and the payee's PSP (or the only PSP) are located within the EEA, irrespective of the currency of the transaction, the rule on charging is that:

- payees must pay any charges levied by their PSP
- payers must pay any charges levied by their PSP

This is also known as a SHARE arrangement.

8.145 The effect of this is that for two leg transactions in any currency, arrangements where the payer pays both their own and the payee's PSPs' charges (known in SWIFT terms

as 'OUR'), or conversely where the payee pays both his, and the payer's PSPs' charges (known in SWIFT terms as 'BEN') are not permitted.

8.146 Any charges levied will be subject to the agreement on charges between the customer and the PSP, in the framework contract or single payment service contract for the payment type concerned.

Charges or reductions for the use of a particular payment instrument (regulation 66(3))

8.147 The payee's PSP cannot prevent the payee from requesting a charge from the payer, or offering a reduction to the payer for, or otherwise steering the payer towards the use of, a particular payment instrument, e.g. credit card, debit card or pre-paid card. Similarly, a merchant cannot be prevented from offering a discount for using a particular payment instrument.

8.148 Where payees are levying additional charges, they need to be aware of their obligations under other legislation, e.g. the Consumer Rights (Payment Surcharges) Regulations 2012.

Authorisation of payment transactions

Consent (regulation 67) and revocation of consent (regulation 83)

8.149 The form and procedure for consent for execution of a transaction to be given by the payer must be set out in the information provided before entering into a framework contract. This should cover both individual transactions and a series of payment transactions (for example, a standing order, direct debit mandate or recurring transaction on a payment card). The PSRs 2017 allow that, where agreed with the customer, consent may be given after the payment transfer has been executed. Otherwise it must be given in advance. Consent may be given via the payee or a PISP.

8.150 Regulation 67 does not define "consent". In our view guidance issued by the Information Commissioner's Office on the meaning of consent in EU data protection law is relevant to the interpretation of Regulation 67 and an act is unlikely to constitute consent for the purposes of regulation 67 unless it is freely given, specific, informed, and there is an indication signifying agreement.

8.151 Regulation 83 sets out the rules on the point from which consent for a particular transaction (as opposed to a series of transactions) may not be revoked by the customer. This will depend on the particular circumstances of the payment transaction in question (eg whether it is an instruction for a future dated payment or an immediate payment). For future dated transactions, up to the agreed point, the customer has a right to withdraw consent to a transaction.

8.152 If consent has been given to a series of payment transactions (for example, a standing order, direct debit mandate or recurring transaction on a payment card) the customer has the right, at any time, to withdraw consent for future transactions in the series. While the PSRs 2017 do not specify how such withdrawal of consent should be given, in our view for payment orders originated by or through the payee (direct debits or recurring transactions), withdrawal of consent notified to either the payer's PSP or to

the payee is valid. The time limits for revocation set out in regulation 83(3) to (5) apply to any payment transaction due within that time period.

8.153 Where consent was given via the payee, it is not acceptable for the payer's PSP to insist that consent may only be withdrawn in the same manner. In our view, any notification to the payer's PSP that the customer wishes to stop payments to a particular payee should be taken as withdrawal of consent to future payments. The PSP may seek clarification of the particular payments to be stopped (if there are more than one to the same payee) and request written confirmation if appropriate, but consent must be taken to have been withdrawn from the time of first notification by the customer.

8.154 In addition, in our view, the closure of an account will amount to withdrawal of consent for any future direct debits or recurring transactions on that account. While it is reasonable for a PSP to say in its terms and conditions that the customer will be liable for any "in flight" transactions (for example, those that have been pre-authorised) that are presented after the closure notification has been received from the customer, we can see no justification for terms that purport to allow PSPs to either effectively keep open an account or re-open previously closed accounts to pay subsequent transactions in the series.

8.155 Unless the PSP can show that consent has been given, it has no authority to make the payment or to debit the customer's account and any such transaction must be regarded as unauthorised. A transaction must also be regarded as unauthorised after consent has been withdrawn.

8.156 The corporate opt-out applies to regulations 67(3) and 67(4), which relate to the withdrawal of consent (see under 'General' at the start of Part II).

Confirmation of availability of funds for card-based payment transactions (regulation 68)

8.157 Regulation 68 provides a mechanism whereby PSPs that issue card-based payment instruments that can be used to initiate a payment transaction from an account held with another PSP (known as the ASPSP) can obtain confirmation of the availability of funds. These issuers are known as card-based payment instrument issuers ("CBPIIs").

8.158 Under regulation 68, CBPIIs can request confirmation from an ASPSP whether a customer has funds available in its account to complete a transaction at a given point in time. However, regulation 68 only governs the confirmation process (i.e. where the ASPSP confirms whether funds are available). It does not govern subsequent settlement of the transaction between the payee, CBPII and the payer, which may vary between different business models. CBPIIs are, therefore, free to agree with their customers whichever model of settlement they choose. CBPIIs will require permission for issuing payment instruments, and further permissions and authorisations may be required depending on how exactly the service is structured. CBPIIs are only permitted to request confirmation of availability of funds if they meet three conditions:

- They have obtained explicit consent from the customer to request the confirmation. In our view, the CBPII should be able to evidence the consent. The CBPII should be clear in its framework contract with the customer how

consent is provided in relation to individual requests for confirmation of availability of funds (eg through the customer entering personalised security credentials at the point of sale) the customer has initiated a transaction using the card-based payment instrument for the amount in question. Consent to initiate such a transaction will be required in accordance with regulation 67.

- the CBPII complies with the requirements of the EBA's Regulatory Technical Standards on strong customer authentication and secure communication (see **Chapter 17 – Payment initiation and account information services and confirmation of availability of funds** for more details about the regulatory technical standards and when they enter into force).
- On receipt of a request meeting the above requirements, the ASPSP is required to provide a yes or no answer on the availability of the amount of funds requested immediately. We consider "immediately" in this context to mean that the response should be sufficiently fast so as not to cause any material delay in the payment transaction.

8.159 On request by the customer, the ASPSP must inform the customer of the request for confirmation and the answer given.

8.160 When providing a yes or no answer, the ASPSP should do so based on whether funds for the execution of the transaction are available. In our view, available funds would include funds covered by an agreed overdraft facility.

8.161 The ASPSP only has to provide confirmation where:

- The account is a payment account which is accessible online for the purpose of giving the yes/no answer. The account does not need to be accessible to the customer to check their balance (see **Chapter 17 – Payment initiation and account information services and confirmation of availability of funds** for more details);
- Before the first occasion on which a request is received, the customer has given their explicit consent to the ASPSP that they can provide confirmation in response to such requests by that CBPII. Consent must be explicit and must relate to the specific CBPII making the request. As a result, in our view it would not be sufficient to include wording in a framework contract to the effect that the customer consents to the ASPSP confirming availability of funds whenever requests come in, nor would any form of "deemed" acceptance be acceptable. The CBPII will, therefore, need to ensure that its customer has given explicit consent to the ASPSP if it wants to obtain confirmation of availability of funds. An ASPSP will need put in place appropriate procedures to ensure that it complies both with its obligations under regulation 67, and its obligations under data protection legislation and regulation 97.

8.162 Regulation 68 does not apply to payment transactions initiated through card-based payment instruments on which e-money is stored. In our view, this only excludes e-money stored on the card itself.

Access to payment accounts for payment initiation services (regulation 69)

8.163 See **Chapter 17 – Payment initiation and account information services and confirmation of availability of funds** for further details.

Access to payment accounts for account information services (regulation 70)

8.164 See **Chapter 17 – Payment initiation and account information services and confirmation of availability of funds** for further details.

Limits on the use of payment instruments and access to payment accounts (regulation 71)

8.165 Before blocking or stopping a payment instrument (for example a debit card or an e-banking service), the PSP must have agreed in the framework contract that it can do so, and must contact the customer to advise them of its intentions and its reason for doing so.

8.166 Stopping or blocking a payment instrument must only be done on reasonable grounds relating to its security, suspected unauthorised or fraudulent use of the payment instrument, or (where the instrument has a credit line) a significantly increased risk the payer may be unable to pay. PSPs may also wish to include wording in their framework contracts advising customers that the payment instrument might be blocked or stopped due to national or EU legal obligations of the PSP. If the PSP is unable to contact the customer beforehand and giving its reasons for blocking or stopping the payment instrument, it must do so immediately after, using the means of communication agreed in the framework contract. However, if providing this information would compromise reasonable security measures, or would be unlawful (for example if it would constitute 'tipping off' under anti-money laundering legislation) this requirement does not apply.

8.167 The PSP is required to unblock the payment instrument, or replace it with a new payment instrument, as soon as practicable after the reasons for blocking cease to apply.

8.168 Regulations 71(2) to 71(5) (which relate to stopping or blocking the payment instrument and notification of this) do not apply where section 98A(4) of the CCA applies. See paragraph 8.141 for further details.

8.169 The parties can also agree to a spending limit on a specific payment instrument. This does not affect the right of a PSP to apply other limits on payments in pursuit of compliance with legislation relating to anti-money laundering, fraud, etc if agreed in the framework contract. This also does not affect the PSP from applying limits on types of transaction (such as limits imposed by the relevant payment scheme) if agreed in the framework contract.

Obligations of the customer in relation to payment instruments and personalised security details (regulation 72)

8.170 The customer is obliged by the PSRs 2017 to abide by the terms and conditions for the use of the payment instrument. However, a customer does not need to abide by any term unless it is objective, non-discriminatory and proportionate. We would consider terms and conditions which, for example, require customers to open and destroy a PIN notification immediately or which prohibit customers from writing down or recording their PIN in any form not to be permitted.

8.171 Terms requiring personalised security details to be kept safe should not be drafted in a way that prevents users from using AIS or PIS, whether expressly or by seeking to shift liability to the customer where such services are used. A PSP cannot use any failure by the customer to abide by such terms as a justification for the customer's liability for unauthorised transactions under regulation 77. Such terms may also be unfair under the CRA or UTTCRs.

8.172 The customer is obliged to notify the PSP, in the agreed manner and without undue delay, should they discover that the payment instrument has been lost or stolen, or that someone else has used (or attempted to use) the payment instrument without the customer's authority.

8.173 The requirement to notify will not apply for low value payment instruments if the nature of the instrument means that it is not possible for the PSP to stop it from being used. (See Part I, section A of this chapter for a definition of low value payment instruments).

8.174 The PSRs 2017 also oblige the customer to take all reasonable steps to keep the personalised security credentials relating to a payment instrument or an account information service safe. This would include the personalised identification number (PIN) or password for the instrument or other piece of information known only to the issuing PSP and the customer. It does not include for example, a credit card number itself, as this would be known to any business where the card was used.

8.175 What constitutes reasonable steps will depend on the circumstances, but PSPs must say what steps they expect customers to take in their pre-contract disclosure information. In line with our view on 'proportionate' contract terms (see paragraph 8.170), we consider that saying that the customer must not write down or record a password or PIN in any form goes beyond "reasonable steps".

Obligations of the PSP in relation to payment instruments (regulation 73)

8.176 The PSP issuing a payment instrument must do the following.

- make sure that any personalised security credentials cannot be accessed by anyone other than the customer involved (subject to the duty of the customer in regulation 72 to keep it safe)
- not send any unsolicited payment instruments to the customer, except as a replacement for the existing payment instrument
- Have appropriate means available at all times (subject to the force majeure provisions of regulation 96) to allow the customer to notify them if the payment instrument is lost, stolen, misappropriated or has been used without the customer's authority, or to request that an instrument be unblocked. This requirement will not apply for low value payment instruments if the nature of the instrument means that it is not possible for the PSP to stop it from being used (see Part I, section A of this chapter for a definition of a low value payment instrument).
- The PSP must be able to provide the customer on request with some way of proving that they have made the notification for 18 months after it has been made; for example this could be by means of providing a reference and by

confirming receipt in writing. This requirement will not apply for low value payment instruments if the nature of the instrument means that it is not possible for the PSP to stop it from being used (see Part I, section A of this chapter for a definition of a low value payment instrument).

- The PSP must provide the customer with a way to notify that a payment instrument is lost, stolen, misappropriated or has been used without the consumer's authority which is free of charge and it must ensure that any costs charged for a replacement payment instrument are directly attributable to replacement. This requirement will not apply for low value payment instruments if the nature of the instrument means that it is not possible for the PSP to stop it from being used (see [Part I, section A] of this chapter for a definition of a low value payment instrument).
- Prevent all use of the payment instrument after having been notified that it has been lost, stolen or misappropriated or used without the customer's authority. Where it is not practically possible in the circumstances to prevent all use of the instrument, transactions generated through the use of the payment instrument should not be debited to the underlying account.

If the PSP sends a payment instrument, PIN, password, etc. to the customer, any risk involved in the sending of the item will remain with the PSP. So, if a card and password were intercepted before they were received by the customer, any losses arising from their misuse would lie with the PSP rather than the customer.

Notification and rectification of unauthorised or incorrectly executed payment transaction (regulation 74)

8.177 If a customer becomes aware of an unauthorised or incorrectly executed payment transaction, they must notify the PSP concerned without undue delay and no later than 13 months after the date of the transaction, or else they will not be entitled to redress under the PSRs 2017.

8.178 ASPSPs, including where a PISP is involved in a transaction. In light of this, and in line with the obligation to provide information under paragraph 5(e) of Schedule 4, we expect ASPSPs to make it clear to customers that notification should be made to the ASPSP in all circumstances (i.e. irrespective of whether a PISP is involved in the transaction).

8.179 It should be noted that PSPs have the ability to grant more favourable terms to their customers, and therefore to offer a longer period (for example, the UK Direct Debit Guarantee Scheme would not be prevented from continuing to offer a longer period for refunds).

8.180 The time limit above will not apply where the PSP has failed to comply with any of the information requirements imposed by the PSRs 2017 in respect of the transaction concerned. Where a payment service is provided in relation to funds covered by a credit line provided under an agreement regulated by the CCA, there are provisions in the CCA which apply in place of this provision.

8.181 For CCA regulated credit cards the PSP must apply the consumer credit regime to all unauthorised transactions instead of regulations 74, 76 and 77 of the PSRs 2017

(although regulation 75 (evidence on authentication and execution of payment transactions) applies). For current accounts with overdrafts, the PSRs 2017 regime will apply in relation to transactions or parts of transactions which occur when the customer is in a credit position and the consumer credit regime in relation to transactions or parts of transactions which occur when the customer is in a debit position.

8.182 Where an unauthorised transaction takes an account from a credit position to an overdrawn position, both regimes will apply (i.e. the PSRs 2017 will apply to the amount that was taken from the credit position and the consumer credit regime will apply to the amount that was taken from the overdraft). In practice this means that PSPs may need to have a different operational process for unauthorised transactions depending on whether the customer is in a credit or debit position, or adopt a process that complies with the minimum standards of both regimes.

8.183 The corporate opt out applies to the time period for notification in this regulation (see under 'General' at the start of Part II of this chapter).

Evidence on authentication and execution of payment transactions (regulation 75)

8.184 Where the customer denies that they have authorised a payment transaction (for example claims that a credit card transaction was not made by them, or claims that a payment transaction has not been correctly executed (for example, if the amount is wrong or has been sent to the wrong place), the obligation lies with the PSP to prove that the payment transaction was:

- authenticated
- accurately recorded
- entered in its accounts
- not affected by a technical breakdown or some other deficiency in the service provided by that PSP

8.185 Where a payment transaction was initiated through a PISP, it is for that PISP to prove that, within its sphere of competence, the payment transaction was:

- authenticated
- accurately recorded
- not affected by a technical breakdown or some other deficiency linked to the payment initiation service

We consider any parts of the transaction over which the PISP has control to be within its "sphere of competence".

8.186 The PSRs 2017 specifically provide that just because the customer's payment instrument has been recorded as having been used, that in itself is not **necessarily** sufficient to prove that the customer authorised the payment, has acted fraudulently, or failed, with intent or gross negligence, to fulfil their obligations in respect of the security of the payment instrument concerned. In our view, since use is only likely to be recorded if any personalised security credentials have been used, this means that providers cannot point to the security features (such as Chip and PIN) alone as

incontestable proof of authorisation, fraud, etc. The corporate opt-out applies to this provision (see under 'General' at the start of Part II of this chapter).

8.187 The effect of this is that, for all customers, other than businesses above micro-enterprise level and charities above small charity[14] level who are able and willing to agree otherwise, each case must be treated on its own merits. Blanket rules in terms and conditions to the effect that the use of the payment instrument will be taken as proper authorisation in all circumstances will not be an effective way of justifying that the customer authorised the payment, or that the customer has acted fraudulently, or failed, with intent or gross negligence, to fulfil their obligations in respect of the security of the payment instrument concerned. Such terms are potentially misleading and may be void under regulation 137(2) of the PSRs 2017 on the basis that they purport to allocate the burden of proof to the customer.

8.188 However, for low value payment instruments, if the nature of the instrument is such that it is not possible for the PSP to prove that it was authorised (for example, if it was used anonymously) this provision will not apply. (See Part I, Section A of this chapter for a definition of low value payment instrument).

PSP's liability for unauthorised transactions (regulation 76)

8.189 If a payment transaction was not properly authorised by the customer, the PSP concerned must refund the amount of the transaction to the payer and, if applicable, restore the relevant payment account to the state it would have been in had the transaction not been made (ie refund any charges and any interest which the customer has paid and/or credit interest which the customer has lost).

8.190 The PSP must also ensure that the credit value date is no later than the date on which the unauthorised amount was debited. We take this to mean that, when the PSP is calculating the amount of interest that should be refunded, the calculation should run from no later than the date the unauthorised amount was debited from the customer's account.

8.191 A transaction should be treated as unauthorised unless the PSP has the consent of the customer as set out in regulation 67. Where an amount has been deducted from a customer's account by a PSP in error, the customer did not consent to this so this should be treated as an unauthorised transaction for the purposes of the PSRs 2017.

8.192 Similarly, where consent has been withdrawn by the customer for either a specific payment transaction or a series of payment transactions, including the payment transaction in question, it should be treated as unauthorised. However, unauthorised transactions can be distinguished from misdirected transactions, where the customer has authorised the transaction but the money has been paid to the wrong recipient. This could be due to the customer providing the incorrect unique identifier (see regulation 90) or it could be the PSP's error (in which case it should be treated as an incorrectly executed transaction under regulations 91 and 92).

[14] see **Glossary of Terms**

8.193 The obligation to provide a refund is subject to any responsibility which the customer may have for the unauthorised transaction under regulation 77.

8.194 A refund must be provided to the customer as soon as practicable and at the latest by the end of the business day following the day on which the PSP becomes aware of the unauthorised transaction (i.e. if a customer notifies the PSP on Monday morning, the refund must be made as soon as practicable and, at the latest, by the end of Tuesday). The only exception to this is where the PSP has reasonable grounds for suspecting fraud and it has notified a person mentioned in s333A(2) of the Proceeds of Crime Act 2002 (e.g. a constable, an officer of HMRC, a nominated officer or an authorised National Crime Agency Officer) in writing. In light of recital 71 to PSD2, we consider 'fraud' in regulation 76 to mean fraudulent behaviour by the payment service user.

8.195 The effect of this is that, in cases where PSPs do not have reasonable grounds to suspect fraud (for example, where the customer may have been grossly negligent), PSPs will nevertheless need to provide a refund by the end of the next business day at the latest and continue any investigation after the refund has been provided.

8.196 It is not appropriate for the PSP to purport to make a refund for an unauthorised transaction conditional on the customer signing a declaration.

8.197 If the results of an investigation enable it to prove either that the customer did authorise the transaction or was otherwise liable, the PSP can reverse the refund. Where this occurs, we would expect the provider to give reasonable notice of the reversal to the customer. What is "reasonable" will depend on the particular circumstances of the case.

8.198 Where the PSP has reasonable grounds to suspect fraud and has made a notification to a person mentioned in s333A(2) of the Proceeds of Crime Act 2002, there is still a balance to be struck between a customer's right to be provided with a refund for an unauthorised payment transaction quickly, and the need to determine whether the payment transaction was fraudulent. We expect PSPs to take a reasonable approach to this.

8.199 Where an investigation is justified, it needs to be carried out as quickly as possible in light of the circumstances. In no circumstances should the investigation be used to discourage the customer from pursuing the claim. Clearly, if such an investigation is carried out and the customer is not found to be at fault, an immediate refund must be made, and back valued so that the customer does not suffer any loss.

8.200 If payment service is provided in relation to funds covered by a credit line provided under an agreement regulated by the CCA then this provision will not apply and consumer credit provisions will apply instead. Regulation 75 requirements (evidence on authentication and execution of payment transactions) do, however, apply and the PSP should also note the provisions of section 171 of the CCA (onus of proof in various proceedings). Our understanding is that this means that unless or until the PSP can provide the evidence to show liability on the part of the customer, the customer is not liable, meaning that no interest should be charged on the disputed amount, and the PSP is not entitled to demand repayment of that sum.

8.201 For low value payment instruments, if the nature of the instrument is such that it is not possible for the PSP to prove that it was authorised (for example, if it was used anonymously) this provision will not apply (See Part I, section A of this chapter for a definition of low value payment instrument).

8.202 Where an unauthorised transaction is initiated through a PISP, it is the ASPSP's responsibility to provide a refund in line with regulation 76 and this guidance. If the PISP is liable, the ASPSP can then seek compensation from the PISP which must, on request, provide that compensation immediately. The amount of compensation should cover the full amount which the ASPSP was required to refund to the customer.

8.203 PSPs are at liberty to offer increased protections to customers in relation to unauthorised transactions and other areas for example through participation in industry schemes such as the Direct Debit Guarantee Scheme. Any such protections apply in addition to the minimum protections that PSPs are obliged to provide under the PSRs 2017.

Customer's liability for unauthorised payment transactions (regulation 77)

8.204 A payment service provider may make its customer liable for losses up to a maximum of £35 resulting from unauthorised transactions from the use of a lost or stolen payment instrument, or from the misappropriation of the payment instrument. It should be noted that the £35 liability limit is applicable to each instance of loss, theft or misappropriation, and not to each transaction. However, this does not apply if:

- it was not possible for the customer to detect the loss, theft or misappropriation before the payment was made (unless the customer acted fraudulently)
- the loss was caused by an employee, agent or branch of a PSP or of an entity which carried out the activities on behalf of the PSP, eg an outsourced provider

The above will not apply for low value payment instruments if the nature of the payment instrument is such that it is not possible for the PSP to prove that it was authorised (for example, if it was used anonymously) (See Part I, Section A of this chapter for a definition of low value payment instrument.

8.205 If the PSP can show that the customer has acted fraudulently, or has intentionally, or with gross negligence, not complied with their obligations under regulation 72 regarding the use of the payment instrument and keeping safe of personalised security credentials, the customer will be liable for all losses. To avoid doubt, it is not sufficient for the PSP to assert that the customer "must have" divulged the personalised security features of the payment instrument, and to effectively require the customer to prove that he did not. The burden of proof lies with the PSP and if a claim that a transaction is unauthorised is rejected, the rejection must be supported by sufficient evidence to prove that the customer is guilty of fraud, gross negligence or intentional breach and the reason for the rejection must be explained to the customer. Regulation 137 provides (amongst other things) that a contractual term is void if and to the extent that it relates to a transaction alleged to have been unauthorised or defectively executed and purports to impose liability to provide compensation on a different person from the person identified in the PSRs 2017, or allocate the burden of proof to a different person from the person identified in the PSRs 2017.

8.206 Each case will need to be assessed on its merits to ascertain whether the customer has acted with 'gross negligence'. In line with the recitals to PSD2, we interpret 'gross negligence' to be a higher standard than the standard of negligence under common law. The customer needs to have shown a very significant degree of carelessness. Except where the payer has acted fraudulently, the payer is not liable for any losses:

- Arising after they notified the PSP of the loss, theft or misappropriation (this will not apply for low value payment instruments if the nature of the instrument means that it is not possible for the PSP to prove that the transaction was authorised – because, for example it is used anonymously - or to stop the payment instrument from being used. See Part I, Section A of this chapter for a definition of low value payment instrument
- if the PSP has failed to provide the means for the payer to make the notification (subject to the force majeure provisions of regulation 96)
- where the payer's PSP does not require strong customer authentication)
- where the payment instrument has been used in connection with a distance contract other than an excepted contract (as defined in the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013

8.207 Where the payee (e.g. a merchant) or the payee's PSP (e.g. the merchant acquirer) does not accept strong customer authentication, the payee or the payee's PSP, or both (as the case may be), must compensate the payer's PSP for the losses incurred or sums paid as a result of it providing a refund to the customer. We expect the payee or payee's PSP to provide the refund within a reasonable period.

8.208 The corporate opt-out applies to this provision (see under "General" at the start of this section).This provision will not apply if the payment service is provided in relation to funds covered by a credit line provided under an agreement regulated by the CCA. See paragraph 8.141 for further details.

Payment transactions where the transaction amount is not known in advance (regulation 78)

8.209 This provision relates to card-based payment transactions where the amount of the transaction is not specified at the point of authorisation. Examples of where this occurs are a credit or debit card pre-authorisation for a hire car or hotel room, for short periods at certain fuel dispensers and when certain online payments are made. In our view, a card-based payment transaction extends further than transactions using a physical card and would include, for example, any payment transaction made by means of a card, telecommunication, digital or IT device or software if this results in a debit card or a credit card or an e-money card transaction.

8.210 For card-based payment transactions where the amount of the transaction is not specified at the point the payer authorises the payment, PSPs must not block funds on the customer's account unless the customer has authorised the exact amount of funds to be blocked.

8.211 Once the PSP becomes aware of the amount of the transaction, it must release the funds without undue delay and, at the latest, immediately after receipt of the payment order.

8.212 We acknowledge that, in some circumstances, a different means of payment is used to settle the transaction than the card on which the funds are blocked (e.g. cash or another payment card). In our view, the obligation to release the blocked funds under regulation 78(b) may not arise in this situation if the PSP does not become aware of the amount of the payment transaction or receive a payment order linked to the blocked funds. However, we still expect PSPs to take a reasonable approach to releasing funds in such circumstances and to do so in accordance with existing industry practice. We understand this to be approximately seven days for credit card transactions and five days for debit card transactions.

8.213 We also suggest that PSPs make clear to customers (whether through contractual documentation or otherwise) the consequences of pre-authorisation. .

Refunds for payment transactions initiated by or through the payee (regulation 79)

8.214 This provision relates to payment transactions that have been initiated by or through the payee (for example, debit or credit card transactions or direct debits), where the exact amount of the transaction was not specified at the point of authorisation (for example, a variable amount direct debit, or a credit or debit card authorisation for a hire car or hotel room). If the amount of the payment transaction exceeds the amount the payer could reasonably have expected in all the circumstances, the payer is entitled to a refund of the full amount of the transaction from their PSP. Those circumstances include the customer's previous spending pattern and the terms of the framework contract, but do not include fluctuations in the reference exchange rate. When providing a refund, the PSP must also ensure that the credit value date is no later than the date on which the payment transaction was debited. In practice, we take this to mean that, when the PSP is providing a refund to the customer of interest lost or paid, the calculation should run from no later than the date the transaction was debited from the customer's account.

8.215 It may be agreed in the framework contract that, if the payer has given their consent directly to their PSP and, if applicable, details of the amount of the transaction have been provided or made available to them at least four weeks before the debit date, they will not have the right to a refund.

8.216 The corporate opt-out applies to this provision (see under "General" at the start of Part II).

8.217 For direct debit transactions which fall within the scope of the Regulation (EU) 260/2012 (that is, SEPA direct debits), the payer is entitled to an unconditional refund from its PSP of the full amount of any authorised direct debit transaction.

8.218 PSPs can agree more favourable terms with their customers. This means that the UK Direct Debit Scheme is at liberty to continue to offer an automatic right to a refund.

Requests for refunds for payment transactions initiated by or through a payee (regulation 80)

8.219 The PSRs 2017 provide that to obtain the refund set out in "Refunds for payment transactions initiated by or through the payee" above, the payer must make their request to the PSP within eight weeks of the debit date. However, PSPs may offer better terms to their customers than those specified in the PSRs 2017. For example, this means that the UK Direct Debit Scheme is at liberty to continue to offer a longer period to request refunds.

8.220 On receipt of a claim for a refund, the PSP may request additional information from the payer, if it is reasonably required to prove whether the conditions have been met. The PSP must either make the refund, or justify refusal within the later of ten days of the claim, or of the additional information being provided. Refusal must be accompanied by information on how to take the matter further if the customer is not satisfied with the justification provided. If the PSP has requested further information, it must not refuse the refund until it has received the information from the customer.

Execution of payment transactions

Receipt of payment orders (regulation 81)

8.221 The point in time of receipt of a payment order, from which the execution time requirements of the PSRs 2017 must be calculated, will generally be the time at which the payment order is received (whether directly or indirectly) by the payer's PSP. The exceptions are as follows:

- that time is not on a business day for that PSP in respect of the particular payment service concerned, in which case the payment order is deemed to have been received on the following business day
- The PSP has set a time towards the end of the business day after which any payment order received will be deemed to have been received on the following business day (notice of this must be given to the customer). It is recognised that this cut-off time may be different, depending upon the requirements of different payment products, but PSPs should take a reasonable approach in setting such cut-off times.
- The customer has agreed with the PSP that the payment order will be executed:
  - on a specific day in the future
  - at the end of a certain period
  - on the day when the payer provides the required funds to the PSP

8.222 Where one of the above applies (i.e. for future dated payments), the agreed date (or, if it is not a business day for the PSP, the next business day) will be deemed to be the time of receipt. This means that the clock starts running for the purposes of the execution time provisions on the agreed date (or, if it is not a business day for the PSP, the next business day).To avoid doubt, it is not possible to "contract out" of this requirement, with either business customers or consumers.

8.223 The aim of the provisions in respect of execution times is to mandate and harmonise the speeding up of payments, so the maximum time taken when neither the payer nor the payee has access to the funds should be one business day. This means, in our view, that

in general where "earmarking" of funds takes place, so that the funds remain in the customer's account for value-dating purposes but are unavailable to the customer to spend, the time of receipt for the purposes of calculating the execution time must be the point at which the funds become unavailable to the customer (i.e. the clock starts running for the purpose of the execution time provisions at the point funds become unavailable).

8.224 In our view, an exception to this can be made in the case of pre-authorisation of card-based payment transactions where the amount is not known in advance (see regulation 78). Here a promise or guarantee of payment has been given by the payer's PSP to the payee, In such cases it may be acceptable, on the basis of recital 77 to the Payment Services Directive 2 and provided the PSP has complied with the requirements of regulation 78, for the funds to be earmarked pending receipt of the actual payment order.

8.225 However, without such a promise or guarantee to the payee, for example in the case of a direct debit or standing order, we can see no justification for earmarking such funds and it is reasonable for the payer to assume they have access to their funds until the date they instructed the direct debit or standing order to be actioned (for example, the first of the month). Similarly, if when sending a Bacs credit the bank earmarked the funds in the payer's account on the day the file was submitted but delayed the debit until the business day before the funds are credited to the payee's PSP's account, the execution time would be longer than "next day" and therefore in breach of the requirements of regulation 86(1).

8.226 The customer's account should never be debited before receipt of the payment order.

8.227 Where the payee's PSP is not reachable by a payment system which enables payments to be made within the prescribed maximum execution times (such as Faster Payments), the provider will need to make alternative arrangements, and clearly explain the position to their customers. Possible options include:

- making the payment through an alternative payment system (eg CHAPS) if available. This must be with the agreement of the customer, who must be advised of (and agree to) any additional charges involved
- Using Bacs, but delaying the debit to the customer's account until, at the earliest, the business day before the Bacs payment will be received by the payee's PSP. This would be classed as a "future dated payment" and the provisions of regulation 81(5) regarding customer agreement will apply. PSPs should also take note of paragraphs 8.223 and 8.225 in respect of 'earmarking'.

8.228 In exceptional circumstances where, in spite of all efforts, it is not possible for the the payment to be made within the specified time limit, PSPs may feel it necessary to refuse the payment order concerned. The requirements of regulation 82 (as set out below) would need to be met in this regard, and where a provider believes that such refusals may be necessary it will need to ensure its framework contracts will need to be amended to allow refusal on these grounds. We would not expect that any such refusal, or notification of a refusal on these grounds, would attract a charge.

8.229 It is expected that PSPs will have made the necessary arrangements to enable their customers to receive payments within the one business day timescale. However, any

PSP whose customer accounts are not reachable by Faster Payments should consider how they will explain to their customers the difficulties that they are likely to experience in receiving payments for their accounts as a result.

Refusal of payment orders (regulation 82)

8.230 A PSP may only refuse to execute a payment order or initiate a payment transaction if the conditions in the framework contract have not been met or execution would be unlawful (for example, in line with anti-money laundering legislation). In line with the recitals to PSD2, customers should be able to rely on the proper execution of the payment order unless the PSP has a contractual or statutory ground for refusal. For ASPSPs, this applies irrespective of whether the payment order is initiated by the customer, through a PISP or by or through a payee.

8.231 Where a PSP refuses to execute a payment order or to initiate a payment transaction, it must notify the customer of the refusal, unless it is unlawful to do so (for example, due to restrictions on tipping-off). The notification must, if possible, include the reasons for the refusal. Where it is possible to provide reasons for the refusal and those reasons relate to factual matters (eg if the customer has not provided the required details to allow the payment to be processed or did not have available funds) the notification must also include what the customer needs to do to correct any errors that led to the refusal. The notification must be provided or made available in the way agreed in the framework contract (for example online) at the earliest opportunity and no later than the end of the next business day following receipt of the payment order.

8.232 Notification need not be provided for low value payment instruments if the non execution is apparent from the context (for example, the purchase is refused at point of sale), (see Part I, section A of this chapter for a definition of low value payment instrument).

8.233 If the refusal is reasonably justified and the framework contract so allows, the PSP may levy a charge for the notification (unless the circumstance set out in paragraph 8.228 applies). This charge must reasonably correspond to the PSP's actual costs. We believe this means that the provider must separately identify any such charge for notification in the framework contract and separately charge this to the underlying account.

Revocation of a payment order (regulation 83)

8.234 The basic rule is that the customer cannot revoke a payment order after it has been received by the payer's PSP. There are, however, some exceptions to the rule:

- For direct debits including recurring transactions on a payment card ('continuous payment authorities') the latest the payer may revoke the payment order is at the end of the business day before the agreed date for the debit. Revocation can be by informing either the payer's PSP or the payee. The effect of withdrawal of consent (in line with regulation 67(4)) is that any future payment transactions are not regarded as authorised. It is an absolute right to withdraw consent from the PSP, and once withdrawn the PSP has no authority to debit the account in question. If the payment order is still processed, the payer would have the right under regulation 76 to an immediate refund from their PSP. However, it is best practice for the customer to be advised that notice of the withdrawal of consent should also be given to the payee, because

revocation of consent to the payment transaction does not affect any continuing obligation of the payer to the payee. For the avoidance of doubt, it is not acceptable for the PSP to purport to make withdrawal of consent dependent upon notice having been given to the payee. This does not affect refund rights after this point through, for example, the Direct Debit Guarantee Scheme.

- For future-dated payments, the latest point at which the payer can revoke the payment instruction is the end of the business day before the day on which payment is due to be made, or if the payment transaction is to be made when funds are available, end of the business day before those funds become available. The use of chip and PIN to pre-authorise a future payment where no order is transmitted to the card issuer at the time of the PIN being entered would not, in our view, affect the payer's right to withdraw consent..
- For other types of payments, if the payment order is initiated by a PISP or by or through the payee (for example a credit or debit card payment) the payer may not revoke the payment order after giving their consent to the PISP to initiate it or to the or payee to execute it (as applicable). So, after entering the PIN on a specific card transaction due for immediate payment the customer cannot revoke the payment order.

8.235 It is important to note that the definition of 'payment transaction' in the PSRs 2017 includes the words 'irrespective of any underlying obligations between the payer and the payee'. The existence, or otherwise, of any obligation of the payer to make payment to the payee does not therefore affect the validity of the withdrawal of consent.

8.236 In our view, where the underlying payment account (e.g. credit card account) has been closed, this is a clear withdrawal of consent for any future transactions that have not already been specifically advised and authorised. We can therefore see no justification for the practice of keeping accounts open or re-opening closed accounts to process recurring transactions received after the account has been closed.

8.237 This will not affect any contractual refund rights the customer may have under the card scheme's own rules, or statutory rights under, for example, section 75 of the Consumer Credit Act.

8.238 For payment orders made direct by the payer to their PSP, revocation later than the limits set out in regulation 83 may be agreed with the relevant PSP or providers. For payment orders initiated by or through the payee (for example, specific payments forming a series of recurring transactions), the agreement of the payee will also be needed to cancel a specific payment where revocation is sought after the end of the business day preceding the day that the specific payment is due to be taken (but such agreement is not needed to withdraw consent to later payments in the series).

8.239 A charge may be made for revocation, if agreed in the framework contract.

8.240 The corporate opt-out applies to this provision (see under "General" at the start of Part II of this chapter).

8.241 For low value payment instruments, the PSP can agree with the customer that the customer cannot revoke the payment order after transmitting it or after giving consent to the payee for the payment transaction (See Part I, section A of this chapter for a definition of low value payment instrument).

Amounts transferred and amounts received – deduction of charges (regulation 84)

8.242 In general, the rule is that the payer and the payee must each pay the charges levied by their own PSP and that no charges can be deducted from the amount transferred.

8.243 The payee can agree with their PSP that it can deduct its charges before crediting the payee, as long as the full amount of the payment transaction and details of the charges deducted are clearly set out in the information provided to the payee. If other charges are deducted, responsibility for rectifying the position and ensuring that the payee receives the correct sum, lies with:

- the payer's PSP, for payments initiated by the payer
- the *payee's PSP, for payments initiated by or through the payee*

Execution time and value date

Applicability (regulation 85)

8.244 The execution time and value dating requirements apply to all:

- payment transactions in euro
- payment transactions executed wholly within the UK in sterling
- payment transactions involving only one currency conversion between sterling and euro where the currency conversion is carried out in the UK and, for a cross-border transfer (that is, a payment transaction where the payer's and the payee's PSPs are located in different member states), the transfer is denominated in euro

8.245 For all other types of transactions, the requirements will apply unless the PSP and its customer agree otherwise (but see also regulation 86(3)). See also the table of jurisdiction and currency in **Chapter 2 – Scope**.

Payment transactions to a payment account – time limits for payment transactions (regulation 86)

8.246 The default rule is that payments have to be credited to the payee's PSP's account (that is the payee's PSP's account with the payment system or where it does not have direct access to the payment system, its own bank or PSP) by close of business on the business day following the day when the payment order was received (or was deemed to have been received – see above under 'Receipt of payment orders').

8.247 An extra day may be added to the above period when the payment order is initiated in paper, rather than electronic form.

8.248 For payment transactions which are to be executed wholly within the EEA (i.e. where both the payer and the payee's PSP are located in the EEA) but which do not fall within regulation 85(1) (see table at paragraph 2.27), the maximum period that may be agreed between the payer's PSP and its customer is the end of the fourth business day following the day on which the payment order was received (i.e. if the payment order was received on Monday, the payment would need to reach the payee's PSP by the end of Friday). This means, for example, that for a payment in Swedish kroner sent from the UK to Sweden, the default position is that the payment would need to be credited to

the payee's PSP by the end of the following business day. However, the payer's PSP can agree with its customer a different timescale although as the payment is to be executed wholly within the EEA, this cannot be longer than the end of the fourth business day following the time of receipt or deemed receipt of the payment order.

8.249 For direct debit transactions and other payments orders initiated by or through the payee, the payee's PSP should transmit the payment order within the time limits agreed between the payee and the PSP so as to allow settlement on the agreed date.

8.250 For merchant acquiring transactions we have included diagrams and an explanatory note setting out one model of how the time limit provisions might work for a four-party card scheme in **Annex 5**. Arguments have been made based on an analysis under UK law of the specific contractual arrangements in some card schemes that an acquirer does not, for the purposes of the PSRs 2017, receive sums for the execution of payment transactions for the benefit of or on behalf of merchants.

8.251 This would have the result that the timescales in regulation 86 to 88 would not apply. The FCA does not, however, agree, with these arguments which would deprive PSD2 of much of its utility in achieving the protection of merchants who receive transfers of funds from acquirers referred to in recital 10 of PSD2. The PSRs 2017 define the 'acquiring of payment transactions' as a payment service "provided by a PSP contracting with a payee to accept and process payment transactions, which results in a transfer of funds to the payee", and this is in line with the FCA's view that the contract between the merchant and the merchant acquirer to which the definition refers involves the execution of payment transactions.

8.252 The payee's PSP must value date and credit the payee's account following receipt of the funds in its own account at the payment system (irrespective of settlement obligations) or if it does not have direct access to the payment system, in its account with its bank or PSP in accordance with regulation 89.

8.253 For low value payment instruments, the PSP can agree with the customer that the execution times in this regulation 86 do not apply (See Part I, section A of this chapter for a definition of low value payment instrument).

Absence of payee's payment account with the PSP (regulation 87)

8.254 Where the payee does not hold a payment account with the PSP (for example, in money remittance services) the PSP to which the payment has been sent must make the funds available immediately after they have been credited to its account. This provision should not be seen as requiring banks which receive funds addressed to a payee for whom they do not hold an account to hold funds pending collection by the payee. In our view it is perfectly acceptable for these funds to be returned to the payer's PSP with the explanation, "No account held".

8.255 For low value payment instruments, the PSP can agree with the customer that the [execution times] in regulation 87 do not apply (See Part I, section A of this chapter for a definition of low value payment instrument).

Cash placed on a payment account (regulation 88)

8.256 Cash placed by a consumer, micro-enterprise or small charity[15] with a PSP for credit to its payment account with that PSP must be credited to the account, value dated and made available immediately after receipt by the PSP. This only applies if the account is denominated in the same currency as the cash. For other customers an extra business day is allowed.

8.257 These time limits apply when cash is paid in at a branch or agent, and whether or not the branch or agent where the cash is paid in is the account holding branch. They will therefore apply, for example to cash paid in to settle a credit card bill, where the card was issued by the bank where the pay in was made.

8.258 Note that where cash is paid to a PSP with instructions for it to be transferred to the customer's account with another, PSP, and the first payment services provider is providing a service to the customer itself — rather than acting as agent for the second PSP — the transaction would be subject to the normal execution time provisions under regulation 86. In these circumstances the use of the paper based credit clearing for such payments would therefore allow an additional day for the credit of the cash to the payee's account.

8.259 In our view, when identifying the point in time at which the cash is deemed to have been received, similar principles to those used in identifying the 'point in time of receipt' for a payment order may be used. This means that, as long as the PSP makes it clear to the customer, the point at which cash is deemed to be received when not taken over the counter by a cashier (for example, left in a nightsafe, or in a deposit box in the branch ("a daysafe")) can be specified in line with reasonable customer expectations as being the point at which the box is opened (for example, the end of the business day for a daysafe and next business day for a nightsafe). In this regard, cash should be distinguished from other types of payments. For other types of payments, the point in time that payments are received (triggering the immediate availability and value dating requirements) should be considered in accordance with regulation 89.

8.260 Where a discrepancy in a cash deposit is discovered after the funds have been credited (for example, counterfeited notes, or the cash has been miscounted) corrections can be made, but corrected post-transaction information will also need to be provided.

Value date and availability of funds (regulation 89)

8.261 The PSRs 2017 in effect prohibit value dating that is detrimental to the customer. This means that the value date of a credit to a payment account can be no later than the business day on which the payment transaction was credited to the payee's PSP's account.

8.262 There are also requirements to make funds available immediately in certain circumstances depending on whether a currency conversion is involved (see the table below). Where the requirement applies, the funds must be at the payee's disposal immediately after they have been credited to the payee's PSP's account.

[15] See **Glossary of Terms**

Type of transaction	Requirement to give immediate availability
Transaction with no currency conversion	Yes
Transaction with a currency conversion between euro and sterling	Yes
Transaction with a currency conversion between two EEA currencies (including sterling and another EEA currency)	Yes
Transaction only involving one PSP	Yes
Any other type of transaction	No requirement to give immediate availability. However, we expect PSPs to act reasonably in the time that it takes to make the funds available. What is reasonable will depend on the currency of the payment that needs to be converted as some currencies take longer to convert than others.

8.263 As soon as the funds are received in the payee's PSP's account, it must make sure that the payee can get access to the funds immediately and credit value date them no later than the business day on which the PSP's account was credited (which includes any account in the PSPs' name). In practice this means that PSPs' systems must identify the funds immediately they are received in their own account and credit them to the payee's account immediately.

8.264 If the time the funds are received is not on a business day, the above requirements will apply at the start of the next business day. A PSP cannot set a "cut-off" time for the receipt of funds that is earlier than the end of the business day. A business day is any day on which the PSP is open for business as required for the execution of a payment transaction. Whether a day is a business day must be considered from the customer's point of view, and will depend upon the individual circumstances of the PSP and is dependent upon the service it provides to its customers.

8.265 For example with respect to a customer with online banking where the customer can make and receive payments at any time using Faster Payments, the PSP is in our view "open for business" 24 hours a day, seven days a week. With respect to a customer with an account which can only be accessed during branch opening hours, those opening hours are likely to represent the "business day". A PSP cannot, whether by contractual terms or otherwise, specify that a day that meets the definition of business day is not to be treated as a business day.

8.266 It is recognised that in practice some processing of the payment by the payee's PSP may be needed before the customer can access the funds. However, the requirement for

"immediate" availability means that the time taken for this processing must be kept to a minimum and we see no reason why, in normal circumstances, this should be longer than two hours. For the avoidance of doubt, unless the payment concerned is received out of business hours, "immediate" can never mean the next business day.

8.267 Payment transactions where both the payer's and the payee's accounts are with the same PSP are within the scope of the PSRs 2017, and as such the execution time provisions will apply. This includes transactions where the payer and the payee are the same person.

8.268 Where a PSP is using its own internal processes to execute the transfer (ie the PSP acts for both the payer and payee), we believe that the principles and aims underlying the execution time provisions in PSD2 and PSRs 2017 must apply, that is, the avoidance of "float" and the efficient processing of payment transactions. We would therefore expect that in such transactions value will be given to the payee on the same day as the payer's account is debited and that the funds will be put at the disposal of the payee immediately.

8.269 Where the payee's account is not a "payment account" and the payee's PSP is a credit institution, the rule in BCOBS 5.1.13 will apply, so that the transaction must be value dated on the business day received, but availability must be within a reasonable period.

8.270 Similarly, debit transactions must not be value dated before the date on which the amount of the debit was debited to the payer's account. For example, in a card transaction, the card issuer cannot value date the debit to the account before the date on which it receives the payment order through the merchant acquiring process (see **Annex 5**).

Liability

Incorrect unique identifiers (regulation 90)

8.271 As part of the information the PSP is required to provide ahead of provision of the payment service, it will specify the 'unique identifier', which is the key information that will be used to route the payment to the correct destination and payee. For UK bank payments in sterling, this is likely to be the sort code number and account number of the payee's account. For SEPA payments it will be the IBAN of the payee. Other information, such as the payee's name or invoice number, may be provided by the payer, but will not be part of the unique identifier, unless it has been specified as such by the PSP.

8.272 The PSRs 2017 provide that, as long as the PSPs process the payment transaction in accordance with the unique identifier provided by the payment service user, they will not be liable under the non-execution or defective execution provisions of the PSRs 2017 for incorrect execution if the unique identifier provided is incorrect.

8.273 The effect of this is if the sort code and account number are quoted as the unique identifier and the account number is incorrect but the account name quoted is correct (so that the funds go to the wrong account), the bank concerned will not be liable under those provisions.

8.274 PSPs are required to make reasonable efforts to recover the funds involved even where they are not liable, but they may, if agreed in the framework contract, make a charge for such recovery. The payee's PSP must co-operate with the payer's PSP in its efforts to recover the funds, in particular by providing all relevant information to the payer's PSP. This co-operation could involve participating in industry schemes relating to the recovery of funds (such as the Credit Payment Recovery Scheme).

8.275 If the PSP is unable to recover the funds and the customer provides a written request, the PSP must, under regulation 90(4), provide to the customer all available relevant information in order for the payer to file a legal claim for repayment of the funds. A PSP may only disclose personal data where it is fair and lawful to do so. When drafting its framework contracts, a PSP should take account of its potential obligations under regulation 90(4) and seek to ensure it is in a position to share the necessary information in a way that is consistent with data protection legislation and its obligations to its customers.

Non-execution or defective or late execution of payment transactions initiated by the payer (regulation 91)

8.276 This provision covers situations where the payer has instructed their PSP to make a payment and the instruction has either not been carried out, or has been carried out incorrectly.

8.277 In these circumstances the payer's PSP will be liable to its customer unless it can prove to the payer (and, where relevant, to the payee's PSP), that the correct amount, and the beneficiary's details as specified by the payer, were received by the payee's PSP on time.

8.278 If it could prove this, the failure to credit the intended payee would then lie with the payee's PSP rather than with itself. If the payer's PSP is liable, it must refund the amount of the defective or non-executed transaction (if such amount has been debited from the payer's account) to the payer without undue delay, and, where applicable, restore the debited payment account to the state it would have been in had the transaction not occurred at all. This may, for example, involve the refunding of charges and adjustment of interest. The PSP must ensure that the credit value date is no later than the date on which the payment transaction was debited. In practice, we take this to mean that, when the PSP is providing a refund to the customer of interest lost or paid, the calculation must run from no later than the date the transaction was debited from the customer's account.

8.279 The effect of this provision is that if, due to the error of the payer's PSP, the funds have been sent to the wrong place or the wrong amount has been sent, as far as the payer is concerned the whole transaction is cancelled. The PSP will either have to stand the loss or seek reimbursement from the other PSP.

8.280 In line with recital 86 of PSD2, which refers to the PSP's obligation to "correct the payment transaction" our view is that to avoid undue enrichment, where an over payment has been made and the excess cannot be recovered from the payee's PSP, it would be appropriate to refund the excess incorrectly deducted from the payer's account where this is sufficient to avoid the payer suffering a loss.

8.281 If the payer's PSP can prove that the payee's PSP received the correct amount and beneficiary details on time, the payee's PSP is liable to its own customer. It must immediately make the funds available to its customer and, where applicable, credit the amount to the customer's payment account.

8.282 The credit value date must be no later than the date on which the amount would have been value dated if the transaction had been executed correctly. In practice, we take this to mean that when the PSP is providing a refund to the customer of interest lost or paid, the calculation must run from no later than the date that the amount would have been value dated if the transaction had been executed correctly.

8.283 Where a payment transaction is executed late, the payer's PSP can request, on behalf of the payer, that the payee's PSP applies a credit value date for the payee's payment account which is no later than the date that the amount would have been value dated if the transaction had been executed correctly. In our view, the aim of this requirement is to ensure that a payee is in the same position as they would have been had the transaction been executed on time (including in respect of charges) and so no claim for late payment will arise against the payer. The payee's PSP can seek recourse from the payer's PSP under regulation 95.

8.284 Liability under this provision will not apply if the failure giving rise to it was due to abnormal and unforeseeable circumstances beyond the control of the relevant PSP, the consequences of which would have been unavoidable despite all efforts to the contrary, or if it arose because of the PSP having to comply with other EU or UK law.

8.285 The corporate opt-out applies to this provision (see under "General" at the start of Part II of this chapter).

8.286 Regardless of liability, if the payer makes a request for information regarding the execution of a payment transaction, its PSP must make immediate efforts to trace the transaction and notify the customer of the outcome. The PSP cannot charge for this.

Non-execution or defective or late execution of payment transactions initiated by the payee (regulation 92)

8.287 This provision covers situations where the payment order has been initiated by the payee (for example, credit or debit card payments, or direct debits), and the instruction has either not been carried out or carried out incorrectly.

8.288 In these circumstances the payee's PSP is liable to its customer unless it can prove to the payee (and, where relevant, to the payer's PSP), that it has carried out its end of the payment transaction properly. That is, it has sent the payment instruction (in the correct amount and within the agreed timescale), and the correct beneficiary details to the payer's PSP, so that the failure to receive the correct amount of funds within the timescale lies with the payer's PSP rather than with itself.

8.289 If it has failed to do this it must immediately re-transmit the payment order. The payee's PSP must also ensure that the credit value date is no later than the date on which the amount would have been value dated if the transaction had been executed correctly. In practice, we take this to mean that the payee's PSP needs to provide a

refund to the customer of interest lost or paid and, in doing so, it must ensure that the calculation runs from no later than the date that the amount would have been value dated if the transaction had been executed correctly.

8.290 If the payee makes a request for information regarding the execution of a payment transaction, their PSP must make immediate efforts to trace the transaction and notify the customer of the outcome. The PSP cannot charge for this.

8.291 If the payer's PSP is liable, its liability is to its own customer rather than the payee, and it must, without undue delay, and as appropriate:

- refund the payer the amount of the payment transaction (for example, if it has been debited and the funds sent to the wrong place)
- restore the debited payment account to the state it would have been in had the transaction not occurred at all

8.292 When it is restoring the payer's account, the payer's PSP must ensure that the credit value date is no later than the date on which the amount was debited. In practice, we take this to mean the calculation must run from no later than the date that the amount was debited from the payer's account.

8.293 If the payer's PSP can prove that the payee's PSP received the amount of the payment transaction, the payee's PSP must value date the transaction no later than the date it would have been valued dated if it had been executed correctly. As above, in practice we take this to mean that the payee's PSP must provide a refund to the customer of interest lost or paid and, in doing so, it must ensure that the calculation runs from no later than the date that the amount would have been value dated if the transaction had been executed correctly.

8.294 As with regulation 91, action short of a full refund may be acceptable, if making a full refund would result in "undue enrichment" to the customer concerned, as long as the customer does not suffer a loss due to the error.

8.295 This may involve the refunding of charges and adjustment of interest. The effect of this provision is that if, due to the error of the PSP, the funds have been sent to the wrong place or the wrong amount has been sent, as far as the payer customer is concerned the whole transaction is cancelled. The PSP will either have to stand the loss or seek reimbursement from the other PSP.

8.296 Liability under this provision will not apply if the failure giving rise to it was due to unavoidable abnormal and unforeseeable circumstances beyond the control of the PSP, the consequences of which would have been unavoidable despite all efforts to the contrary, or if it arose because of the PSP having to comply with other EU or UK law.

Non-execution or defective or late execution of payment transactions initiated through a payment initiation service (regulation 93)

8.297 Where a payment transaction initiated through a payment initiation service has either not been carried out, or has been carried out incorrectly, it is the ASPSP's responsibility to provide a refund of the amount of the transaction to the customer and, where applicable, to restore the account to the state it would have been in if the defective payment transaction had not taken place.

8.298 If the PISP is responsible, on request from the ASPSP, it must immediately compensate the ASPSP for all losses incurred or sums paid as a result of the refund to the customer.

8.299 The burden of proof lies with the PISP to show that it was not responsible for the error. It needs to prove that the payment order was received by the customer's ASPSP and, within the PISP's sphere of influence, the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency. We consider any parts of the transaction over which the PISP has control to be within its sphere of influence.

Liability of PSP for charges and interest (regulation 94)

8.300 A PSP that is liable for non-execution, defective execution or late execution of a payment transaction under the provisions detailed above will also be liable to its customer for any resulting charges and/or interest incurred by the customer. For example, if a customer was making a payment to a credit card account from their current account, and the provider of the current account was responsible for executing the payment transaction late, that customer would be entitled to a refund for any charges and interest applied to the their credit card account. This liability will not be incurred if the circumstances giving rise to it were due to abnormal and unforeseeable circumstances beyond the control of the PSP.

8.301 The corporate opt-out applies to this provision (see under "General" at the start of Part II of this chapter).

Right of recourse (regulation 95)

8.302 If a PSP has incurred a loss or been required to make a payment with respect to unauthorised transactions, or the non-execution, defective execution, or late execution of a payment transaction, but that liability is due to the actions of another PSP or an intermediary, the other PSP or intermediary must compensate the first PSP. This includes compensation where any of the payment services providers fail to use strong customer authentication

Force majeure (regulation 96)

8.303 Liability under the conduct of business requirements in Part 7 of the PSRs 2017 relating to rights and obligations (but not to the information requirements in Part 6) will not apply where the liability is due to:

- abnormal and unforeseen circumstances beyond the person's control, where the consequences would have been unavoidable despite all efforts to the contrary
- obligations under other provisions of EU or national law (for example, anti-money laundering legislation)

Consent for use of personal information (regulation 97)

8.304 A PSP must not access, process or retain any personal information for the provision of payment services unless it has the explicit consent of its customer to do so. PSPs should also be aware of their wider obligations under data protection law and regulation in relation to the processing of personal data.

Part III: Additional conduct of business requirements for e-money issuers

8.305 This section includes some additional conduct of business rules applicable to all e-money issuers, including those authorised under FSMA.

8.306 We are aware that a number of pre-paid cards have been issued in the UK by "programme managers" which utilise e-money issued by a credit institution or e-money issuer. Under these arrangements, the programme manager manages the card and takes transaction and other fees from the card user, but the underlying funds are held by the e-money issuing institution. In our view the e-money issuer will usually be the PSP for the purposes of the PSRs 2017, given that the programme manager does not hold any customer funds.

8.307 The arrangement will fall under the outsourcing provision in regulation 26 of the EMRs or under SYSC 8 for credit institutions issuing e-money, and may, depending on the business model, involve agency or distribution arrangements. In the situation described, the e-money issuer is therefore responsible for ensuring that the conduct of business requirements set out in this chapter are complied with.

The conduct of business requirements in the EMRs

8.308 Part 5 of the EMRs sets out obligations that apply to the conduct of e-money business where it is carried out from an establishment maintained by an e-money issuer or its agent or distributor in the UK. These are typically referred to as conduct of business requirements. They relate to issuing and redeeming e-money and the prohibition on the payment of interest or other benefits linked to the length of time that e-money is held and are applicable to all e-money issuers (see **Chapter 2 – Scope** for the definition of e-money issuers).

Issuing e-money

8.309 Regulation 39 requires e-money issuers to issue e-money at par value (the e-money issued must be for the same amount as the funds received) when they receive the funds and without delay.

8.310 It is important to recognise that if an agent of an e-money issuer receives funds, the funds are considered to have been received by the issuer itself. It is not, therefore, acceptable for an e-money issuer to delay in enabling the customer to begin spending the e-money because the issuer is waiting to receive funds from its agent or distributor.

Redeeming e-money

8.311 Under the EMRs, e-money holders have the right to redeem the monetary value of their e-money (that is the payment from the e-money issuer to the e-money holder of an amount equivalent to the remaining balance) at any time and at par value (regulation 39).

8.312 This means that, in our view, it is not acceptable to have a term in a contract with an e-money holder under which the e-money holder's right to redeem the remaining balance ceases to apply after a specified period of validity (although the contract can still provide for the e-money holder's right to use the e-money for the purpose of making payment transactions to cease after a specified period). This is qualified by regulation

43 which allows e-money issuers to refuse a redemption request when the request is made more than six years after the date of termination in the contract.

8.313 The contract between the e-money issuer and the e-money holder must, clearly and prominently, set out the conditions of redemption (or part thereof), including any fees that may be payable. E-money holders must be advised about these conditions before they are bound by the contract.

Redemption fees

8.314 If it is agreed and transparent in the contract, e-money issuers may charge a fee for redemption in the following circumstances:

- where redemption is requested before termination of the contract
- where the e-money holder terminates the contract before any agreed termination date
- where redemption is requested more than one year after the date of termination of the contract

8.315 For these purposes, references to the termination of the contract refer to the point in time when the e-money holder's right to use the e-money for the purpose of making payment transactions ceases.

8.316 The effect of this is that no fee for redemption may be charged to the e-money holder on requesting redemption at termination of the contract or up to one year after that date. In this chapter, we use the phrase "dormant e-money" to describe e-money held more than one year after the termination of the contract.

8.317 Any fee that is charged should be proportionate and in line with the costs actually incurred by the e-money issuer. In our view, it is reasonable for the calculation of a redemption fee to take account of costs the issuer can show it actually incurs in retaining records of and safeguarding dormant e-money (on the basis that any such costs must relate to redemption rather than making payments). If challenged, the e-money issuer must be able to justify the level of the fee charged by reference to costs that it has incurred, either in the act of redeeming the dormant e-money, or in retaining records of and safeguarding the dormant e-money.

8.318 In principle, we do not consider that it would be objectionable for an issuer to deduct from the proceeds of redemption of dormant e-money the amount of any redemption fee (as long as the e-money issuer can demonstrate that the redemption fee is clear and prominent in the contract and reflects only valid redemption-related costs). So, if the amount of a valid redemption fee is greater than the value of the dormant e-money, in practice the proceeds of any redemption by the holder would be nil, after the fee is deducted.

8.319 In these circumstances, it would be reasonable for the issuer to cease to safeguard those dormant e-money funds (as there is no utility in requiring issuers to safeguard dormant e-money funds that can no longer be spent or redeemed). The issuer would, however, have to be able to show to the e-money holder that this is how the e-money balance has been used up, in the event of the e-money holder later seeking redemption.

8.320 The above guidance on redemption does not apply to a person (other than a consumer) who accepts e-money (for example, a merchant who has accepted e-money in payment for goods or services). For such persons, redemption rights will be subject to the contractual agreement between the parties.

Prohibition of interest

8.321 E-money issuers are not allowed to grant interest or any other benefits related to the length of time the e-money is held. In our view this would not prohibit benefits related to spending levels.

9. Capital resources and requirements

9.1 This chapter describes the capital resources and requirements for authorised PIs, authorised EMIs and small EMIs. It is not relevant to small PIs or RAISPs. The PII requirements that will apply to firms carrying on AIS and PIS are covered in **Chapter 3 – Authorisation and registration**. This chapter covers:

- Requirements for authorised PIs
  - Introduction
  - Initial capital requirements
  - Ongoing capital requirements

- Requirements for authorised EMIs and small EMIs
  - Introduction
  - Initial capital requirements
  - Ongoing capital requirements

Requirements for authorised PIs

Introduction

9.2 The PSRs set out initial and ongoing capital requirements for authorised PIs. Under the PSRs, authorised PIs are required to hold a minimum amount of capital. Capital is required to be held as a buffer, absorbing both unexpected losses that arise while a firm is a going concern as well as the first losses if a firm is wound up.

9.3 Regulations 6(3), 22, and Schedule 3 of the PSRs 2017 cover capital resources and requirements. We have to maintain arrangements such as monitoring so that we can ascertain whether the capital requirements are being complied with as required. These are described in **Chapter 12 - Supervision**.

9.4 The term ‘capital resources’ describes what a firm holds as capital.

9.5 The term ‘capital requirements’ refers to the amount of capital that must be held by the firm for regulatory purposes. The PSRs 2017 establish initial capital requirements (which are a condition of authorisation) and ongoing capital requirements. An authorised PI must at all times hold the capital amounts required, in the manner specified. The capital requirements set out in the PSRs 2017 are expressed in euro. Firms should hold sufficient capital to ensure that the capital requirements are met, even in the event of exchange rate fluctuations. Current and historical rates can be found on the European Commission's InforEuro website.

9.6 Authorised PIs can undertake activities that are not related to providing payment services. These businesses are called ‘hybrid’ businesses. The PSRs do not impose any initial or ongoing capital requirements in relation to the business that does not involve payment services. Any other capital requirements imposed because of other legislation – for example, if the PI is undertaking an activity regulated under FSMA – have to be

met separately and cumulatively. An authorised PI must not include in its capital calculations any item also included in the capital calculations of another authorised PI, credit institution, investment firm, asset management company or insurance undertaking within the same group. Also, where an authorised PI carries out activities other than providing payment services, it must not include in its capital calculation items used in carrying out the other activities.

Initial capital requirements

9.7 The initial capital requirement is one of the conditions to be met at the application stage in order for the authorised PI to become authorised by us. The PSRs 2017 set out that the initial capital requirement of authorised PIs will be €20,000, €50,000 or €125,000 depending on the business activities carried out by the firm (see table below). Where more than one initial capital requirement applies to an authorised PI, it must hold the greater amount.

9.8 RAISPs do not have to meet any initial capital requirements.

9.9 The items that may be used to meet the initial capital requirements are set out in Article 26(1)(a) to (e) of Regulation (EU) 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 ('the Capital Requirements Regulation'). Additional sources of information about the Capital Requirements Regulation can be found at:

- European Commission: Capital Requirements - CRD IV/CRR - Frequently Asked Questions: and the general web page on CRD/CRR
- European Banking Authority: Single Rulebook
- The FCA's CRD IV web page

9.10 The minimum initial capital required is as follows:

Payment Services (see Schedule 1 to the PSRs 2017)	Initial Capital Required (Minimum)
Money remittance (paragraph 1(f) of Part 1, Schedule 1 of the PSRs 2017)	€ 20,000
Payment initiation services (paragraph 1(g) of Part 1, Schedule 1 of the PSRs 2017)	€ 50,000
Account information services (paragraph 1(h) of Part 1, Schedule 1 of the PSRs 2017)	None
Payment institutions providing services covered in paragraphs 1 (a) to (e) of Part 1, Schedule 1 of the PSRs 2017	€ 125,000

Ongoing capital (or 'own funds') requirements

9.11 Subject to the below, authorised PIs are required to hold at all times 'own funds' equal to or in excess of the greater of:

- the amount of initial capital required for its business activity; or
- in the case of authorised PIs other than those that carry on only PIS, the amount of the own funds requirement calculated in accordance with Method A, B or C (described in more detail below), subject to any adjustment we require.

9.12 Authorised PIs should look to the Capital Requirements Regulation to understand the items that may be used to calculate 'own funds' which are defined in Article 4(1)(118) of the Capital Requirements Regulation as funds where at least 75% of the Tier 1 capital is in the form of Common Equity Tier 1 capital (as referred to in Article 50 of the Capital Requirements Regulation) and Tier 2 capital is equal to or less than one third of Tier 1 capital. You should refer to the sources in paragraph 9 for more information on the Capital Requirements Regulation.

9.13 There is no own funds requirement for:

- RAISPs; and
- authorised PIs that are included within the consolidated supervision of a parent credit institution pursuant to Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 relating to the activity of credit institutions and the prudential supervision of credit institutions and investment firms ('the Capital Requirements Directive') and where all of the conditions specified in Article 7(1) of the Capital Requirements Regulation have been met. They must, however, still ensure that they continue to hold the amount of initial capital required for their business activity at all times.

Calculation of ongoing capital (or 'own funds') requirements

9.14 There are three methods of calculation for the own funds requirements. This section explains the three methods (methods A, B, and C).

9.15 The authorised PI will be asked, in the application pack, to indicate which calculation method it wishes to use. However, we must ultimately direct which method is to be used (based on our evaluation of the authorised PI), taking the firm's preference into account.

Method A

9.16 Calculation method A is based on the firm's fixed overheads. The calculation is normally 10% of the preceding year's fixed overheads. However, if there is a material change in the firm's business since the preceding financial year, we may decide that the requirement is higher or lower than 10%. Examples of material changes include the sale of parts of the business, a business acquisition and rapid growth (typically of a new business).

9.17 Fixed overheads are defined as including expenses that do not vary as a result of output volume or sales revenue. For example rent, insurance and office expenses. General accounting standards should be followed in valuing the specific expenses to be taken into account. Only expenses that are related to payment services should be taken into account when calculating the fixed overheads of firms which also provide services other than payment services (hybrid firms).

Method B

9.18 Method B is based on a scaled amount representing the firm's average monthly payment volume and then applying a scaling factor relevant to the type of payment services carried out (see the table below at [9.12] for the relevant scaling factor). Under this calculation method, the firm's ongoing capital requirement is the product of this scaling factor and the scaled average monthly payment volume. The scaled average monthly payment volume is the total amount of the PI's payment transactions executed in the previous financial year divided by the number of months in that year scaled in the following manner:

- (a) 4% of the slice of the average monthly payment volume up to €5 million,
- (b) 2.5% of the slice of the average monthly payment volume above €5 million up to €10 million,
- (c) 1% of the slice of the average monthly payment volume above €10 million up to €100 million,
- (d) 0.5% of the slice of the average monthly payment volume above €100 million up to €250 million, and
- (e) 0.25% of the average monthly payment volume above €250 million.

Method C

9.19 Method C is based on the firm's income over the preceding year with a scaling factor applied. The firm's income is derived by applying a multiplication factor to income described as the 'relevant indicator' in the PSRs 2017. Here, the income is the sum of the firm's interest income, interest expenses, commission and fees received as well as other operating income.

9.20 These are defined as:

- 'interest income' – interest received by the authorised PI from the investments it has made whether or not made from the users' funds.
- 'interest expenses – interest payable by the authorised PI to its creditors or users where the funds stay on its payment accounts.
- 'commission and fees received' – these should be expressed in gross.
- 'other operating income' - any other kind of income which, in the case of a non-hybrid firm, may be linked to payment services or ancillary services (as set out at regulation 32) – these should be expressed in gross.

9.21 The multiplication factor applied to the relevant indicator is the sum of:

- 10% of income up to €2.5 million;
- 8% of income between €2.5 million and €5 million;
- 6% of income between €5 million and €25 million;
- 3% of income between €25 million and €50 million; and
- 1.5% of income above €50 million.

9.22 The scaling factor applied to methods B and C is based on the type of service provided, and is the higher of the following:

Payment services (from paragraph 1 of Schedule 1 of the PSRs 2017)	**Scaling Factor**
Money remittance services only (paragraph 1(f) of Part 1, Schedule 1 of the PSRs 2017)	0.5
Any payment service specified in paragraphs 1(a) to (e) of Part 1, Schedule 1 of the PSRs 2017.	1.0

9.23 When calculating the ongoing capital requirement, if a PI has not completed a financial year of business, the figure for the preceding financial year should be taken as the projected figure which the firm has submitted in its business plan provided as part of the PI's application for authorisation (subject to any adjustments that we have required).

9.24 We may direct an authorised PI to hold capital up to 20% higher or 20% lower than the outcome of its ongoing requirement calculation, based on our evaluation of the authorised PI. The evaluation may take into account risk management processes, risk loss database or internal control mechanisms, if available and as we consider appropriate. We may make a reasonable charge for this evaluation. The details are set out in paragraphs 4 to 6 of Schedule 3 of the PSRs 2017.

Application of accounting standards

9.25 Where there is a reference to an asset, liability, equity or income statement, the authorised PI must recognise that item and measure its value in accordance with the following (as applicable to the authorised PI for its external financial reporting):

- Financial Reporting Standards and Statements of Standard Accounting Practice issued or adopted by Financial Reporting Council Limited;
- Statements of Recommended Practice issued by industry or sectoral bodies recognised for this purpose by Financial Reporting Council Limited;
- International Financial Reporting Standards and International Accounting Standards issued or adopted by the IASB;
- International Standards on Auditing (UK and Ireland) issued by Financial Reporting Council Limited or a predecessor body; and
- The Companies Act 2006.

The exception is where the PSRs provide for a different method of recognition, measurement or valuation.

Requirements for authorised EMIs and small EMIs

Introduction

9.26 The EMRs establish capital requirements for EMIs and some small EMIs. Under the EMRs, authorised EMIs and those small EMIs whose average outstanding e-money exceeds the relevant monetary threshold are required to hold a minimum amount of capital. Capital is required to be held as a buffer, absorbing both unexpected losses that arise while the business is a going concern as well as the first losses if it is wound up. The parts of the EMRs that deal with the capital resources and requirements are regulations 6(3), 13(5), 19 and Schedule 2. We will monitor whether the capital requirements are being complied with as required. Our supervisory approach is described in **Chapter 12 - Supervision**.

9.27 The term 'capital resources' describes what a business holds as capital.

9.28 The term 'capital requirements' refers to the amount of capital that must be held by the business for regulatory purposes. The capital requirements established by the EMRs are (i) initial capital requirements that are a condition of authorisation or registration and (ii) ongoing capital requirements. EMIs must at all times hold the capital amounts required, in the manner specified. The capital requirements set out in the EMRs are expressed in euro. It is expected that EMIs will hold sufficient capital to ensure that the capital requirements are met, even in the event of exchange rate fluctuations. Current and historical rates can be found on the European Commission's InforEuro website.

9.29 EMIs can also provide payment services that are unrelated to the activity of issuing e-money. There are separate capital requirements for authorised EMIs that provide such unrelated payment services.

9.30 Additionally, EMIs can undertake activities that are not related to issuing e-money and payment services at all. These businesses are called 'hybrid' businesses. The EMRs do not impose any initial or ongoing capital requirements in relation to the business that does not involve issuing e-money or providing payment services. Any other capital requirements imposed because of other legislation – for example, if the EMI is undertaking an activity regulated under FSMA – have to be met separately and cumulatively.

9.31 For the purposes of calculating the capital requirements, EMIs that provide unrelated payment services or that are hybrid businesses must treat each part of the business separately.

Initial capital requirements

9.32 The initial capital requirement is one of the conditions to be met at the application stage. The EMRs specify the following initial capital requirements:

- authorised EMIs must hold at least €350,000; and

- small EMIs whose business activities generate (or are projected to generate) average outstanding e-money of €500,000 or more must hold an amount of initial capital at least equal to 2% of their average outstanding e–money.

9.33 There is no initial capital requirement for small EMIs whose business activities generate (or are projected to generate) average outstanding e-money less than €500,000.

9.34 If the applicant for small EMI status does not have a sufficient period of business history to calculate average outstanding e-money then projected amounts (as outlined in their business plan) may be used, subject to any adjustments we may require.

9.35 The items that may be used to meet the initial capital requirement are set out in Article 26(1)(a) to (e) of the Capital Requirements Regulation.

Ongoing capital (or 'own funds') requirements

E-money issuing business

9.36 Authorised EMIs are at all times required to hold 'own funds' equal to or in excess of the greater of:

- the amount of initial capital required for its business activity (i.e. €350,000); or
- the amount of the own funds requirement calculated in accordance with Method D (as described in more detail below) in respect of any activities carried on that consist of the issuance of e-money and payment services related to the issuance of e-money, subject to any adjustment we require.

9.37 Authorised EMIs should look to the Capital Requirements Regulation to understand the items that may be used to calculate 'own funds' which are defined in Article 4(1)(118) of the Capital Requirements Regulation as funds where at least 75% of the Tier 1 capital is in the form of Common Equity Tier 1 capital (as referred to in Article 50 of that Regulation) and Tier 2 capital is equal to or less than one third of Tier 1 capital.

9.38 Small EMIs subject to an initial 2% capital requirement must continue to meet this on an ongoing basis unless their level of business falls below the threshold.

Unrelated payment services business

9.39 If an authorised EMI chooses to provide unrelated payment services (i.e. those not related to its e-money issuing activities) it must meet separate and additional ongoing capital requirements for this part of the business. The authorised EMI does not have to meet any additional initial capital requirements for the unrelated payment services.

9.40 The ongoing capital requirements for unrelated payment services are laid out in paragraph 13(a) of Schedule 2 to the EMRs and correspond to Methods A, B and C as detailed above in paragraphs [9.4 – 9.14].

9.41 Authorised EMIs that provide unrelated payment services are asked in the application pack to indicate which calculation method they wish to use. We will direct (based on

our evaluation of the authorised EMI) which method is to be used, taking into account the authorised EMI's preference.

9.42 Small EMIs are allowed to provide payments services not related to the issuance of e-money on the same basis as a small PI. There are no initial or ongoing capital requirements for small EMIs in relation to their unrelated payment services business.

9.43 An authorised EMI that undertakes business other than issuing e-money and providing related payment services must not use:

- in its calculation of own funds in accordance with methods A, B or C, any qualifying item included in its calculation of own funds in accordance with method D;
- in its calculation of own funds in accordance with method D, any qualifying item included in its calculation of own funds in accordance with methods A, B or C; or
- in its calculation of own funds in accordance with methods A, B, C or D any qualifying item included in its calculation of own funds to meet its capital requirement for any other regulated activity under FSMA or any other enactment.

Calculating ongoing capital ('own funds') requirements for e-money business

9.44 A description of Methods A, B and C (for the unrelated payment services business) is set out above. Method D (for the e-money business) is set out below.

9.45 Authorised EMIs that have not completed six months of the e-money business or a financial year for the unrelated payment services business should use the projected figure submitted in their business plan in their application for authorisation (subject to any adjustments we require).

9.46 We may direct an authorised EMI or small EMI to hold capital up to 20% higher or permit it to hold capital up to 20% lower than the outcome of its ongoing requirement calculation for its e-money business or its unrelated payment services activities (or both), based on our evaluation of the authorised or small EMI. The evaluation may take into account risk management processes, risk loss database or internal control mechanisms (if available and as we consider appropriate). We may make a reasonable charge for this evaluation. The details are set out in Schedule 2 of the EMRs

Method D

9.47 Method D is 2% of the average outstanding e-money issued by the EMI.

9.48 The "average outstanding e-money" for the purposes of Method D is the average total amount of financial liabilities related to e-money in issue at the end of each calendar day over the preceding six calendar months. This figure must be calculated on the first calendar day of each calendar month and applied for that calendar month (i.e. calculations and adjustments must be made monthly), as set out in regulation 2 of the EMRs. It is not sufficient for EMIs to calculate the average outstanding e-money on a bi-annual basis.

9.49 As referred to above, EMIs that have not completed a sufficiently long period of business to calculate the amount of average outstanding e-money for these purposes should use the projected figure submitted in the business plan in their application for authorisation (subject to any adjustments that we have required).

9.50 If an authorised EMI provides payment services that are not related to issuing e-money or is a hybrid business and the amount of outstanding e-money is not known in advance, the authorised EMI may calculate its own funds requirement on the basis of a representative portion being assumed as e-money, as long as a representative portion can be reasonably estimated on the basis of historical data and to the satisfaction of the FCA. Where an authorised EMI has not completed a sufficiently long period of business to compile historical data adequate to make that calculation, it must make an estimate on the basis of projected outstanding e-money as evidenced by its business plan, subject to any adjustments to that plan which are, or have been, required by the FCA.

Applying accounting standards

9.51 Where there is a reference to an asset, liability, equity or income statement item, the authorised EMI must recognise that item and measure its value in accordance with the following (as set out in paragraph [25], Schedule 2 of the EMRs):

- Financial Reporting Standards and Statements of Standard Accounting Practice issued or adopted by Financial Reporting Council Limited;
- Statements of Recommended Practice, issued by industry or sectoral bodies recognised for this purpose by Financial Reporting Council Limited;
- International Financial Reporting Standards and International Accounting Standards issued or adopted by the IASB;
- International Standards on Auditing (UK and Ireland) issued by Financial Reporting Council Limited or a predecessor body; and
- the Companies Act 2006.

9.52 The exception is where the EMRs or PSRs provide for a different method of recognition, measurement or valuation.

10. Safeguarding

Introduction

10.1 This chapter explains the safeguarding requirements for authorised PIs, authorised EMIs, small EMIs and credit unions that issue e-money and their responsibility to ensure appropriate organisational arrangements are in place to protect the safeguarded funds. These businesses are reminded that adequate safeguarding measures are a pre-requisite for being granted and retaining an authorisation for the provision of payment and e- money services. This chapter also sets out the obligations that small PIs must comply with, if they choose to voluntarily safeguard.

10.2 The obligation to safeguard starts **immediately** on receipt of funds ('relevant funds' see 10.14 -10.17 below).

Safeguarding funds from payment services under the PSRs 2017

10.3 All authorised PIs are required to comply with the safeguarding requirements in regulation 23 of the PSRs 2017.

10.4 Small PIs can choose to comply with the safeguarding requirements in the PSRs 2017 in order to offer the same protections over customer funds as authorised PIs must provide. If a small PI does choose to safeguard it will need to apply the same level of protections as are expected of an authorised PI, as described in this chapter. We expect a small PI to tell us if it is choosing to safeguard funds, both in its application for registration and in annual reporting returns.

10.5 If a small PI decides to begin safeguarding funds after it has been registered, or alternatively, if a small PI which has advised us that it has chosen to safeguard at the time of registration decides that it will cease doing so, it should advise us of this as soon as possible through the Customer Contact Centre.

Safeguarding funds received in exchange for e-money under the EMRs

10.6 All authorised EMIs and small EMIs are required by regulation 20 of the EMRs to safeguard funds received in exchange for e-money that has been issued.

10.7 A credit union that issues e-money will have a Part 4A permission under FSMA to issue e-money but is required under the EMRs to safeguard funds received in exchange for e-money as if it were an EMI (regulation 20(5) of the EMRs).

Safeguarding funds from unrelated payment services under the EMRs

10.8 EMIs and credit unions that issue e-money are also entitled to provide payment services that are unrelated to the issuance of e-money (regulation 20(6) of the EMRs).

10.9 Authorised EMIs that provide unrelated payment services are subject to the safeguarding provisions of the PSRs 2017 (regulation 23 of the PSRs 2017) as if they were authorised PIs.

10.10 Small EMIs that provide unrelated payment services are in the same position as small PIs with respect to safeguarding. Under the PSRs 2017 small PIs can choose to comply with the safeguarding requirements in the PSRs 2017 for funds received for payment services in order to offer the same protection over customer funds as authorised EMIs and authorised PIs must provide. If a small EMI chooses to safeguard funds received for unrelated payment services it will have to deliver the same level of protection as is expected of an authorised EMI and authorised PI, as described in this chapter. We require businesses applying to become small EMIs that provide unrelated payment services to tell us if they will safeguard these funds. Those that opt to safeguard funds received for unrelated payment services will have to provide information about their safeguarding arrangements in annual reporting returns.

10.11 Credit unions that issue e-money and provide unrelated payment services are subject to regulation 23 of the PSRs 2017 on the same basis as small EMIs.

10.12 We refer to authorised PIs, authorised EMIs, small EMIs, credit unions that issue e-money and small PIs (when subject to voluntary safeguarding requirements) as "institutions" throughout this chapter.

Purpose of safeguarding

10.13 The PSRs 2017 and EMRs impose safeguarding requirements to protect customers where funds (see 10.14) are held by an institution. They do this by ensuring that those funds are either placed in a separate account from the institution's working capital and other funds or are covered by an appropriate insurance policy or comparable guarantee. On the insolvency of an institution, claims of e-money holders/payment service users are paid from the asset pool formed from these funds in priority to all other creditors (other than in respect of the costs of distributing the asset pool).

What funds need to be safeguarded?

10.14 The requirement to safeguard applies to 'relevant funds' in both the PSRs 2017 and EMRs.

10.15 Under the EMRs, relevant funds are funds that have been received in exchange for e-money that has been issued. Relevant funds received in the form of payment by a payment instrument only have to be safeguarded when they are credited to the EMI's or credit union's payment account or are otherwise made available to the EMI or credit union, subject to the requirement that they are safeguarded by the end of five business days after the date on which the e-money was issued. This relates to e-money paid for by a payment instrument such as a credit or debit card and not e-money that is paid for by cash.

10.16 Authorised EMIs must also separately safeguard relevant funds received in relation to unrelated payment services. Small EMIs and credit unions may choose to safeguard relevant funds received in relation to unrelated payment services. Regulation 23 of the PSRs 2017 applies to these funds.

10.17 Under the PSRs 2017, relevant funds are:

- sums received from, or for the benefit of, a payment service user for the execution of a payment transaction; and
- sums received from a payment service provider for the execution of a payment transaction on behalf of a payment service user.

10.18 This means that safeguarding extends to funds that are not received directly from a payment service user, but includes, for example, funds received by an institution from another PSP for the institution's payment service user. Some institutions receive funds from the public in respect of other services. Examples include:

- an EMI with a foreign exchange business,
- a foreign exchange business that also provides money transmission services and
- a telecommunications network operator which receives funds from the public both for the provision of its own services (for example airtime) and for onward transmission to third parties.

10.19 The EMRs and PSRs 2017 safeguarding requirements only apply to relevant funds. However, sometimes such businesses will not know the precise portion of relevant funds and funds received in relation to the non-payment service provided, or the amount may be variable. In these circumstances, an institution may make a reasonable estimate on the basis of relevant historical data of the portion that is attributable to e-money/the execution of the payment transaction and so must be safeguarded. The institution would, if asked, need to supply us with evidence that the proportion actually safeguarded was a reasonable estimate. Relevant data might include the portion generally attributable to e-money/payment transactions by the customer in question or by similar customers generally.

10.20 In our view, an institution that is carrying out a foreign exchange transaction independently from its payment services is not required by the PSRs 2017/EMRs to safeguard funds received for the purpose of the foreign exchange transaction (see Q12 in PERG 15.2). Indeed, where an institution is using the segregation method of safeguarding (see below), the foreign exchange transaction funds will need to be kept separate from the payment service transaction funds as they are not relevant funds. Once the foreign exchange transaction has taken place, if the institution pays those funds on to a third party on behalf of its client, and this amounts to a payment service, the currency purchased in the foreign exchange transaction becomes relevant funds to be safeguarded as soon as it is received by the institution. To be clear, in our view, in making a payment of currency to its customer in settlement of a foreign exchange transaction, the FX provider will be acting as principal in purchasing the other currency from its customer. This does not constitute a payment service.

10.21 It is possible that the FX transaction could be subject to the second Markets in Financial Instruments Directive (MiFID II) (see PERG 13 Q31K). The institution would thereby have to comply with the client money requirements in CASS 7 of the FCA Handbook until the currency purchased in the FX transaction is received for the execution of a payment transaction. CASS client money should be segregated from relevant funds.

10.22 Institutions combining payment and non-payment services will need to be clear in their prior information to customers about whether, when and in what way, funds will be

protected and about precisely which services benefit from this protection, to avoid breaching the Consumer Protection for Unfair Trading Regulations 2008.

10.23 Institutions which operate outside the EEA should note that transactions where both the payer and the payee are outside the EEA (for example a transfer between Japan and Hong Kong) are outside the scope of the safeguarding provisions of the PSRs 2017, and as such, funds received for these transactions should not be included in segregated funds. Where the payer, the payee and their PSP are all outside the EEA, the transaction is outside of scope even if one of the PSPs routes funds through a correspondent PSP in the EEA.

10.24 It is important that the availability of an asset pool from which to pay the claims of e-money holders or payment service users in priority to other creditors in the event of the insolvency of an institution is not undermined by the institution improperly mixing funds, assets or proceeds received or held for different purposes. For example, if an account that an institution holds with an authorised credit institution is used not only for holding funds received in exchange for e-money/for the execution of payment transactions but also for holding fees due to the business or funds received for other activities (such as foreign exchange), this carries a significant risk of corrupting the asset pool, and may result in the protection for payment service users in regulation 24 of the EMRs or regulation 23 of the PSRs 2017 not applying. As a further illustration, an institution may safeguard relevant funds by covering them with an insurance policy or comparable guarantee. However, if the account into which the proceeds of the policy or guarantee are payable is also used for holding funds for other activities, or for holding the proceeds of another insurance policy taken out to safeguard funds received for another purpose, then this may mean that the proceeds are not considered to be an 'asset pool' subject to the special rules about the priority of creditors in the event of an insolvency.

When does the obligation to safeguard start and end?

10.25 The safeguarding obligation starts as soon as the institution receives the funds. For an institution accepting cash, for example in the provision of money remittance services, the funds will be received as soon as the cash is handed over. In our view, an institution will have received funds as soon as it has an entitlement to them. This could include an entitlement to funds in a bank account in the customer's name, funds in an account in the customer's name at another institution and funds held on trust for the customer.

10.26 For an institution receiving funds through a payment system, if they are required, by the rules of that system or the availability provision in regulation 89 of the PSRs 2017, to make funds available to the payee from a particular point in time, in our view it is likely that the safeguarding obligation will start no later than that point. We expect that this will generally be the same point in time at which the funds are credited to the institution's account with the payment system.

10.27 The general principle is that the safeguarding obligation remains in place until the funds are no longer held by the institution. In practice, this means that the institution should generally continue to safeguard until funds are paid out to the payee or the payee's payment service provider. If a chain of PSPs is involved, the funds must always be

safeguarded for the benefit of the payer or payee; it is not sufficient for the funds to be safeguarded for the benefit of another PSP in the payment chain.

10.28 An institution may receive and hold funds through an agent or (in the case of EMIs and small EMIs) a distributor. The institution must safeguard the funds as soon as funds are received by the agent or distributor and continue to safeguard until those funds are paid out to the payee, the payee's PSP or another PSP in the payment chain that is not acting on behalf of the institution. The obligation to safeguard in such circumstances remains with the institution (not with the agent or distributor). Institutions are responsible, to the same extent as if they had expressly permitted it, for anything done or not done by their agents or distributors (as per regulation 36 in the EMRs and regulation 36 in the PSRs 2017).

How must funds be safeguarded?

10.29 There are two ways in which an institution may safeguard relevant funds:

- the segregation method and
- the insurance or comparable guarantee method.

An institution should choose one method and should not combine them.

10.30 We expect institutions to notify us if they intend to change which method they use to safeguard funds in line with their obligation to notify a change in circumstances under regulation 17 of the EMRs or regulation 32 of the PSRs 2017.

The segregation method

10.31 The first method requires the institution to segregate the relevant funds i.e. keep them separate from all other funds it holds and, if the funds are still held at the end of the business day following the day on which they were received, to deposit the funds in a separate account with an authorised credit institution or the Bank of England (references in this chapter to safeguarding with an authorised credit institutions include safeguarding with the Bank of England, unless the context requires otherwise), or to invest the relevant funds in such secure, liquid assets as we may approve and place those assets in a separate account with an authorised custodian.

Requirement to segregate

10.32 Institutions must segregate i.e. keep relevant funds separate from other funds that they hold as soon as those funds are received. It would not be sufficient to segregate funds in the institution's books/records; if held electronically, the funds must be held in a separate account at a third party account provider, such as a credit institution. Funds held in banknotes and coins must be physically segregated.

10.33 There may be instances where, for customer convenience, the institution receives funds from customers that include both relevant funds and fees owed to the institution. However, this increases risk to relevant funds. We expect institutions to segregate the relevant funds by removing them into a segregated account as frequently as practicable

throughout the day. In no circumstances should such funds be kept commingled overnight.

10.34 Where relevant funds are held on an institution's behalf by agents or distributors, the institution remains responsible for ensuring that the agent or distributor segregates the funds.

Requirement to deposit relevant funds in a separate account with an authorised credit institution or invest them in secure, liquid assets

10.35 If relevant funds continue to be held at the end of the business day following the day that the institution (or agent/distributor) received them, the institution must:

- deposit the relevant funds in a separate account that it holds with an authorised credit institution or the Bank of England; or
- invest the relevant funds in secure, liquid assets approved by us and place those assets in a separate account with an authorised custodian.

10.36 An authorised credit institution includes UK banks and building societies authorised by us to accept deposits (including UK branches of third country credit institutions) and EEA firms authorised as credit institutions by their home state competent authorities.

10.37 Authorised custodians include firms authorised by us to safeguard and administer investments and EEA firms authorised as investment firms under MiFID II and which hold investments under the standards in Article 16 of MiFID II.

10.38 The safeguarding account in which the relevant funds or equivalent assets are held must be named in a way that shows it is a safeguarding account (rather than an account used to hold money belonging to the institution). If it is not possible for a particular EEA authorised credit institution to make the necessary designation evident in the name of the account, we expect the institution to provide evidence (e.g. a letter from the relevant credit institution) confirming the appropriate designation. The account must be in the name of the institution and not an agent or distributor.

10.39 The safeguarding account must not be used to hold any other funds or assets. For EMIs/credit unions that are safeguarding funds received for both e-money and unrelated payment services, the funds should not be held in the same safeguarding account.

10.40 No one other than the institution may have any interest in or right over the relevant funds or assets in the safeguarding account, except as provided by regulation 24 of the EMRs and regulation 23 of the PSRs 2017. The institution should have an acknowledgement or otherwise be able to demonstrate that the authorised credit institution or authorised custodian has no rights (for example, of set off) or interest (for example, a charge) over funds or assets in that account.

10.41 In our view, one effect of this is that institutions cannot share safeguarding accounts. For example, a corporate group containing several institutions cannot pool its respective relevant funds or assets in a single account. Each institution must therefore have its own safeguarding account.

10.42 The EMRs/PSRs 2017 do not prevent institutions from holding more than one safeguarding account.

10.43 The EMRs/PSRs 2017 also do not prohibit the same account being used to segregate funds up to the end of the business day following receipt, and to continue to safeguard the funds from that point onwards, as long as the account meets the additional requirements of the safeguarding account.

10.44 We expect that almost all institutions will, at some point, hold funds after the end of the business day following receipt. Even if an institution only holds funds in this way on an exceptional basis, those institutions will still need to hold a safeguarding account. If an institution believes that, due to its business model, it does not need to have a safeguarding account in place, the institution should ensure that it has appropriate evidence to prove that it will never hold relevant funds after the end of the business day following receipt.

Secure, liquid assets the FCA may approve

10.45 Where an institution chooses to invest relevant funds into assets, regulations 23(5)(b) of the PSRs 2017 and 21(6)(a) of the EMRs require that any such assets are approved by us as being secure and liquid. We use a common approach for the PSRs 2017 and the EMRs in identifying suitable assets. We have approved the assets referred to below as liquid. On this basis, these assets are both secure and liquid, and institutions can invest in them and place them in a separate account with an authorised custodian in order to comply with the safeguarding requirement, if they are:

- items that fall into one of the categories set out in Article 114 of the Capital Requirements Regulation (EU 575/2013) for which the specific risk capital charge is no higher than 0%; or
- units in an undertaking for collective investment in transferable securities (UCITS), which invests solely in the assets mentioned previously.

10.46 An institution may request that we approve other assets. We will make our decision on a case by case basis, with the institution being required to demonstrate how the consumer protection objectives of safeguarding will be met by investing in the assets in question.

10.47 We may, in exceptional cases, determine that an asset that would otherwise be described as secure and liquid is not in fact such an asset, provided that:

- such a determination is based on an evaluation of the risks associated with the asset, including any risk arising from the security, maturity or value of the asset; and
- there is adequate justification for the determination.

The insurance or guarantee method

10.48 The second safeguarding method is to arrange for the relevant funds to be covered by an insurance policy with an authorised insurer, or a comparable guarantee given by an

authorised insurer or an authorised credit institution. The policy or comparable guarantee will need to cover all relevant funds, not just funds held by an institution at the end of the business day following the day that they were received.

10.49 It is important that the insurance policy or comparable guarantee meets the requirements of the EMRs/PSRs 2017. In particular, a suitable guarantee would not be a 'guarantee' in the way that this is often construed under English law (i.e. where the guarantor assumes a secondary liability to see that the institution pays a specified debt or performs an obligation and becomes liable if the institution defaults). The guarantor must assume a primary liability to pay a sum equal to the amount of relevant funds upon the occurrence of an insolvency event (as defined in regulation 24 of the EMRs and regulation 23 of the PSRs 2017). As such, we do not think it is appropriate or desirable to use a term such as "surety" to describe the type of obligation assumed under the arrangements.

10.50 There must be no other condition or restriction on the prompt paying out of the funds, accepting that some form of certification as to the occurrence of an insolvency event is a practical necessity. Where relevant funds are safeguarded by insurance or comparable guarantee, it is important that the arrangements will achieve, at the earliest possible time after the PI is subject to an insolvency event, the same sum standing to the credit of the designated account as would be the case if the PI had segregated the funds all along.

10.51 The proceeds of the insurance policy or comparable guarantee must be payable into a separate account held by the institution. The account must be named in a way that shows it is a safeguarding account rather than an account used to hold money belonging to the institution. The account must not be used for holding any other funds. No-one other than the institution may have an interest in or right over the proceeds of the policy or guarantee (except as provided for by regulation 24 of the EMRs and regulation 23 of the PSRs 2017).

10.52 The arrangements must ensure that the proceeds of the insurance policy or comparable guarantee fall outside of the institution's insolvent estate, so as to be protected from creditors other than payment service users or e-money holders. In our view, one way of achieving this is for the insurance policy or comparable guarantee to be written in trust for the benefit of the payment service users or e-money holders from the outset and to also declare a trust of the designated account

10.53 If EMIs/credit unions use this method for relevant funds received in exchange for e-money and relevant funds received for unrelated payment services, they must ensure that the insurance policy(ies) or comparable guarantee(s) cover both sets of funds and provide for them to be paid into separate accounts.

10.54 An 'authorised insurer' means a person authorised for the purposes of FSMA to effect and carry out a contract of general insurance as principal or otherwise authorised in accordance with Article 14 of Directive 2009/138/EC (Solvency II)[16] to carry out non-

[16] of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance

life insurance activities as referred to in Article 2(2) of that Directive, other than a person in the same group as the authorised institution.

10.55 Neither the authorised credit institution nor the authorised insurer can be part of the corporate group to which the institution belongs.

Systems and controls

10.56 Institutions must maintain organisational arrangements that are sufficient to minimise the risk of the loss or diminution of relevant funds or assets through fraud, misuse, negligence or poor administration (regulation 24(3) of the EMRs and regulation 23(14) of the PSRs 2017). This requirement is in addition to the general requirements on institutions to have effective risk management procedures, adequate internal control mechanisms and to maintain relevant records.

10.57 An institution's auditor is required to tell us if it has become aware in its capacity as an auditor that, in its opinion, there is or has been, may be or may have been, a breach of any requirements imposed by or under the PSRs 2017/EMRs that is of material significance to us (regulation 25 of the EMRs and regulation 24 of the PSRs 2017). This includes a breach of the safeguarding requirements and the organisational arrangements requirement. For EMIs, this may be in relation to either or both the issuing of e-money and the provision of unrelated payment services.

10.58 In our view, arrangements that institutions should have in place include the following:

- Institutions should maintain records that are sufficient to show and explain their compliance with all aspects of their safeguarding obligations. This should include a documented rationale for every decision they make regarding the safeguarding process and the systems and controls that they have in place. Such decisions should be reviewed regularly.

- Institutions should ensure an appropriate individual within the institution has oversight of all procedures relating to safeguarding and responsibility for ensuring that every aspect of the safeguarding procedure is compliant.

- Institutions should exercise all due skill, care and diligence in selecting, appointing and periodically reviewing credit institutions, custodians and insurers involved in the institution's safeguarding arrangements. Institutions should take account of the expertise and market reputation of the third party and any legal requirements or market practices related to the holding of relevant funds or assets that could adversely affect e-money holders' or payment service users' rights or the protections afforded by regulation 20 of the EMRs and regulation 23 of the PSRs 2017 (for example where the local law of a third country credit institution holding a safeguarding account would not recognise the priority afforded by the EMRs and PSRs 2017 to e-money holders/payment service users on insolvency). Institutions should also consider, together with any other relevant matters:

    - the need for diversification of risks;
    - the capital and credit rating of the third party;

- the amount of relevant funds or assets placed, guaranteed or insured as a proportion of a third party's capital and (in the case of a credit institution) deposits; and
- the level of risk in the investment and loan activities undertaken by the third party and its affiliates (to the extent that information is available).

when it makes its decision on appropriateness, an institution should record the grounds for that decision.

- Institutions should have arrangements to ensure that relevant funds held by persons acting on their behalf (such as agents or distributors) are safeguarded in accordance with regulation 20 of the EMRs and regulation 23 of the PSRs 2017.

- In order to ensure it is clear what funds have been segregated and in what way, institutions must keep records of any:

  - relevant funds segregated;
  - relevant funds placed in an account with an authorised credit institution; and
  - assets placed in a custody account.

- An institution's records should enable it, at any time and without delay, to distinguish relevant funds and assets held:

  - for one e-money holder/payment service user from those held for any other e-money holder/payment service user and
  - for one e-money holder/payment service user from its own money. The records should be sufficient to show and explain the institution's transactions concerning relevant funds and assets.

- Records and accounts should be maintained in a way that ensures accuracy and corresponds to the amounts held for e-money holders/payment service users.

- An institution should carry out internal reconciliations of records and accounts of the entitlement of e-money holders/payment service users to relevant funds and assets with the records and accounts of amounts safeguarded. This should be done as often as necessary, and as soon as reasonably practicable after the date to which the reconciliation relates, to ensure the accuracy of the institution's records and accounts. Records should be maintained that are sufficient to show and explain the method of internal reconciliation and its adequacy.

- An institution should regularly carry out reconciliations between its internal accounts and records and those of any third parties safeguarding relevant funds or assets. Reconciliations should be performed as regularly as is necessary and as soon as reasonably practicable after the date to which the reconciliation relates to ensure the accuracy of its internal accounts and records against those of the third parties. When determining whether the frequency is adequate, the institution should consider the risks to which the business is exposed, such as

the nature, volume and complexity of the business, and where and with whom the relevant funds and assets are held.

Reconciliation

10.59 Certain permitted forms of safeguarding give rise to the potential for discrepancies between the amount safeguarded and the amount that should be safeguarded that are very difficult to completely avoid. Examples of this are:

- where relevant funds are invested in secure, liquid assets;
- where relevant funds are held in a currency other than the currency of the payment transaction;
- where payment service users do not pay sums for the execution of payment transactions directly into a safeguarding account, out of which payment transactions are then executed, but rather the institution ensures that a net amount equivalent to relevant funds is segregated and (where regulation 23 (5) applies) held in a safeguarding account.

10.60 Where such a potential for discrepancies exists, reconciliation should be carried out as often as is practicable. In no circumstances would it be acceptable for reconciliation to be carried out less than once during each business day. The reconciliation should result in the amount of funds or assets safeguarded being

- sufficient to cover the amount that the institution would need to safeguard before the next reconciliation and
- (not excessive (to minimise risks arising from commingling).

10.61 The institution's approach to reconciliation must be supported by a clear explanation and must be signed off by the institution's board of directors. The explanation should also make clear that all funds or assets in the segregated or safeguarded account (as applicable) are held for the benefit of payment service users / e-money holders within the meaning of the PSRs 2017/ EMRs (as applicable).

10.62 Where relevant funds are held in a currency other than the currency of the payment transaction, the reconciliation should be carried out using an appropriate exchange rate such as the previous day's closing spot exchange rate.

10.63 We consider an adequate method of reconciliation is for a comparison to be made and any discrepancies identified between:

- the total balance of relevant funds as recorded by the institution with the total balance on all safeguarding accounts as set out on the statement or other form of confirmation issued by the authorised credit institution or custodian holding the account; and
- the total balance on the e-money holders'/payment service users' transaction accounts as recorded by the institution, with the total balance on all safeguarding accounts, as set out in the statement or other form of confirmation issued by the authorised credit institution or custodian that holds the account.

10.64 Where discrepancies arise as a result of reconciliations, institutions should identify the reason for those discrepancies and correct them as soon as possible by paying in any shortfall or withdrawing any excess, unless the discrepancy arises only due to timing differences between internal and external accounting systems. In no circumstances would it be acceptable for corrections to be made after the end of the business day. Where a discrepancy cannot be immediately resolved, institutions should assume that the records that show that a greater amount of relevant funds or assets should be safeguarded are correct, until the discrepancy is resolved. Institutions should be able to demonstrate that they are carrying out appropriate reconciliations and correcting discrepancies.

10.65 Institutions should notify us in writing without delay if in any material respect they have not complied with or are unable to comply with the requirements in regulation 20 of the EMRs or regulation 23 of the PSRs 2017, or if they cannot resolve any reconciliation discrepancies in the way described.

Effect of an insolvency event

10.66 If an insolvency event (listed in regulation 24 of the EMRs or regulation 23(15) of the PSRs 2017, as appropriate) occurs in relation to an institution then, with one exception, the claims of e-money holders/payment services users will be paid from the relevant funds and assets that have been segregated (the 'asset pool') in priority to all other creditors. The exception is that expenses of the insolvency proceedings take priority so far as they are in respect of the costs of distributing the asset pool.

10.67 No right of set-off or security right can be exercised in respect of the asset pool, except to the extent that it relates to the fees and expenses in relation to operating a safeguarding account.

11. Complaint handling

11.1 This chapter summarises complaint handling requirements that apply to all payment service providers and e-money issuers.

Introduction

11.2 Complaint handling covers three areas:

- how payment service providers and e-money issuers handle the complaints they receive from customers (including record keeping and reporting complaints to us)
- the role of the Financial Ombudsman Service dealing with complaints where customers are not satisfied with the payment service provider's/e-money issuer's response
- our role in handling complaints from customers and other interested parties about alleged breaches of the PSRs 2017 and the EMRs, and about the FCA

Handling complaints from customers

11.3 It is important that businesses have their own complaints-handling arrangements. Those arrangements should resolve most complaints.

11.4 The rules on handling complaints from eligible complainants are not set out in the PSRs 2017 or the EMRs. They are set out in the Dispute Resolution: Complaints sourcebook (DISP) in our Handbook. DISP sets out the meaning of eligible complainants and we also provide details in this chapter at paragraph 11.34.

11.5 All payment service providers and e-money issuers are subject to the dispute resolution rules in DISP, even if they are not required to be authorised or registered by us. For guidance on the persons that are defined as payment service providers and e-money issuers see **Chapter 2 - Scope**.

11.6 The rules in DISP cover a range of issues, including:

- consumer awareness
- internal complaint-handling procedures
- timeliness
- the requirement for a final-response letter
- the rules on referral of complaints to others
- cooperation with the Financial Ombudsman Service

11.7 In some cases, the rules in DISP are different to the rules that apply to activities that are not payment services activities or the issuance of e-money. This includes the rules relating to consumer awareness and complaints handling time limits.

11.8 The rules for handling complaints about the rights and obligations under Parts 6 and 7 of the PSRs 2017 from non-eligible complainants are set out in regulation 101 of the PSRs 2017.

Providing information about complaints procedures

11.9 The PSRs 2017 require payment service providers to provide information about the availability of alternative dispute resolution procedures for payment service users and how to access to them as part of their pre-contractual information (see, regulations 43 and 48 and paragraph 7(b) of Schedule 4 to the PSRs 2017). This will also apply to the payment service element of e-money issuers business.

11.10 This means informing users about the payment service provider's own complaints mechanism, the availability of the Financial Ombudsman Service — or where the complainant is not an eligible complainant, another dispute resolution provider — and any other alternative dispute resolution procedures (such as under the Online Dispute Resolution Regulations (EU 524/2013)). in these ways:

- for single payment transactions, this information must be made available 'before the payment service user is bound by the single payment service contract'
- for framework contracts, this information must be provided 'in good time before the payment service user is bound by the framework contract'

11.11 In both cases, where the contract is concluded using distance means the information can be provided immediately after conclusion of the contract — or immediately after the execution of the transaction for single payment service contracts — if the method used to conclude the contract does not enable earlier provision. The information required under the PSRs 2017 can be provided using the summary details required under DISP 1.2.

11.12 Payment service providers and e-money issuers are subject to the complaints handling rules in DISP 1.2 when dealing with complaints from eligible complainants. DISP 1.2 is modified to take account of the information requirements under the PSRs.

11.13 The requirements for payment services are therefore different in terms of content and timing from the requirements in DISP 1.2 for other types of business. For other types of business, the payment service provider or e-money issuer should refer eligible complaints to the availability of these summary details at or immediately after the point of sale or, in relation to a payment service, at the branch where the service is provided. Where the activity does not involve a sale, this obligation applies at or immediately after the point when contact is first made with an eligible complainant.

11.14 This means payment service providers who also undertake other types of business that we regulate have to operate different arrangements for payment service users and other customers. If they want to, payment service providers can apply the requirements for payment service users to all their customers, since they also satisfy the requirements set out in DISP 1.2 for all customers.

Complaints handling time limits

11.15 Article 101 PSD2 sets out time limits for handling complaints. For eligible complainants these are implemented by our rules in DISP.

11.16 DISP 1.6.2A requires payment service providers and e-money issuers to send a final response to complaints about rights and obligations arising under Parts 6 and 7 of the PSRs 2017 — a PSD complaint— and Part 5 of the EMRs — an EMD complaint — by the end of 15 business days after the day on which it received the complaint (or, in exceptional circumstances, by the end of 35 business days after the day on which it received the complaint).

11.17 These time limits are different to those that apply to complaints about other aspects of the payment service or e-money. They are also different to complaints about other types of business we regulate, which are subject to the time limit requirements in DISP1.6.2.

11.18 Payment service providers and e-money issuers are, therefore, subject to different complaints time limits depending on whether the complaint is a PSD complaint or EMD complaint or not. If they want to, payment service providers and e-money issuers can apply the DISP 1.6.2A time limits to all of their complaints from customers, since they satisfy the requirements set out in DISP 1.6 for other complaints.

11.19 The time limit rules in DISP 1.6 do not apply to a complaint resolved by close of business on the third business day following the day on which it is received (see DISP 1.5).

11.20 For PSD complaints from complainants that are not eligible complainants, regulation 101 of the PSRs 2017 requires payment service providers and e-money issuers to respond to complaints within 15 business days or, in exceptional circumstances, 35 business days.

Complaints recording and reporting

11.21 Payment service providers and e-money issuers must keep a record of each complaint they receive and the measures taken for its resolution, and retain that record for three years - see DISP 1.9.

11.22 Credit institutions, PIs and EMIs must provide us with an annual report on complaints received about payment services or e-money. See DISP 1.10B, the complaints reporting directions. Credit institutions, PIs and EMIs must follow the instructions on the GABRIEL system to submit their returns electronically.

11.23 The complaints reporting directions apply to all complaints from payment service users, whether or not they are eligible complainants (i.e. those within the scope of regulation 101 PSR as well as DISP 1) and to complaints from e-money holders that are eligible complainants.

11.24 The requirements in the complaints reporting directions are in addition to other complaints reporting requirements that apply to FSMA authorised firms. Firms should refer to DISP 1.10 for further details.

The role of the Financial Ombudsman Service in dealing with complaints

11.25 The Financial Ombudsman Service operates the out-of-court complaint and redress procedures for payment services and e-money holders that are eligible complainants required by PSD2 and EMD.

11.26 Financial Ombudsman Service is a statutory, informal dispute-resolution service, established under FSMA and independent of the FCA. It operates as an alternative to the civil courts. Its role is to resolve disputes between eligible complainants and financial services firms quickly, without taking sides and with minimum formality, on the basis of what is fair and reasonable in the circumstances of each case.

11.27 The Financial Ombudsman Service looks at the relevant law, regulations, regulators' rules, guidance and standards, relevant codes of practice and, where appropriate, what it considers to have been good industry practice at the relevant time.

11.28 Where a complaint about the rights and obligations under Parts 6 and 7 of the PSRs 2017 is from a payment service user that is not an eligible complainant, regulation 101 of the PSRs 2017 requires the payment service provider to inform the payment service user of at least one provider of dispute resolution services which is able to deal with its complaint. As the payment service user will not be able to make a complaint to the Financial Ombudsman Service they will need to be informed of a dispute-resolution service such as a commercial dispute resolution service with which the payment service provider has an agreement.

Jurisdiction of the Financial Ombudsman Service

11.29 There are two separate jurisdictions under the Financial Ombudsman Service:

- The compulsory jurisdiction covers all firms, authorised or registered and regulated by the FCA and a limited number of other financial services businesses. All payment service providers and e-money issuers with UK establishments are subject to the compulsory jurisdiction.
- The voluntary jurisdiction. This covers financial services businesses that are not covered by the compulsory but choose to join the voluntary jurisdiction, for instance payment service provider and e-money issuers providing services in the UK from overseas.

11.30 All payment service providers and e-money issuers with UK establishments are covered by the CJ for disputes concerning the provision of payment services, issuance of e-money and credit-related regulated activities, and activities ancillary to those activities.

11.31 Complaints can be made about payment service providers and e-money issuers that no longer provide payment services or issue e-money. Former payment service providers and former e-money issuers remain in the compulsory jurisdiction for complaints about an act or omission that occurred when they provided payment services or issued e-money, as long as the compulsory jurisdiction rules were in force at the time the activity took place.

11.32 Further information about the Financial Ombudsman Service's processes for handling complaints is available on its website.

11.33 There is also information specifically for smaller businesses.

Eligible complainants

11.34 The full details of who is eligible to bring a complaint are set out in DISP 2.7. In summary, access to the Financial Ombudsman Service is available to:

- consumers
- micro-enterprises (see paragraph 11.30)
- small charities with annual income under £1 million at the time of the complaint
- small trusts with net asset value under £1 million at the time of the complaint
- CBTL consumers (in relation to CBTL business)
- A business may not bring a complaint about an activity that it conducts itself. This extends to complaints from e-money issuers about payment service provision, as all e-money issuers are also entitled to provide payment services.

11.35 If a payment service provider or e-money issuer is in any doubt about the eligibility of a complainant, it should treat the complainant as if it were eligible. If the complaint is referred to the Financial Ombudsman Service, it will determine eligibility by reference to appropriate evidence, such as accounts or VAT returns in the case of micro-enterprises.

11.36 A micro-enterprise is an business which both:

- employs fewer than 10 people
- has a turnover or annual balance sheet that does not exceed €2 million

11.37 When calculating turnover or balance sheet levels, the European Commission's monthly accounting rate of the euro may be used[17].

11.38 For a complaint about payment services or e-money, the complainant is eligible if it is a micro-enterprise either at the point of concluding the contract or at the time of the complaint. The point of this 'dual test' is to make it easier for firms to determine whether the complainant is eligible. Payment service providers and e-money issuers should have arrangements in place to check whether their customers are micro-enterprises at the time of conclusion of the contract. However, if this information is not easily available, the dual test would allow a complainant instead to rely on its status at the time of making the complaint.

11.39 For other activities covered by the Financial Ombudsman Service's jurisdiction, the test for eligibility is whether the complainant is a micro-enterprise "at the time the complainant refers the complaint to the respondent". This is in line with the eligibility tests for small charities and trusts.

[17] The European Commission provides a tool to calculate the monthly accounting rate of the Euro here: http://ec.europa.eu/budget/contracts_grants/info_contracts/inforeuro/index_en.cfm

11.40 The dual test means that where the complaint is about a number of issues, including payment services, the firm may only have to consider eligibility at the time the complaint was made. However, if the complainant was not eligible at the time the complaint was made and the case appears borderline, it will also be necessary to investigate the complainant's status at the point of concluding the contract.

Transitional arrangements for small business complainants

11.41 Until 1 November 2009, small businesses with a group turnover of under £1 million per year were eligible to take complaints to the Financial Ombudsman Service. The implementation of PSD1 resulted in a change to the eligibility criteria, meaning that some small businesses that until that date had been eligible to take complaints to the Financial Ombudsman Service lost that right from 1 November 2009. In order to protect the position of these small businesses, the old eligibility test continues to apply, if necessary, for complaints about any policy or contract taken out before 1 November 2009 where the payment service provider was subject to the Financial Ombudsman Service's jurisdiction before that date.

Territorial scope of the compulsory jurisdiction for complaints against payment service providers and e-money issuers

11.42 The compulsory jurisdiction covers complaints about the payment services, e-money and ancillary activities of a firm carried on from an establishment in the UK. This includes EEA-authorised PIs' and EMIs' UK branches or agents.

Cross-border disputes

11.43 The Financial Ombudsman Service co-operates with dispute resolution services in other EEA countries to resolve cross-border disputes. The Financial Ombudsman Service is a member of FIN-NET, the financial dispute resolution network of national out-of-court complaint schemes in the EEA.

The voluntary jurisdiction of the Financial Ombudsman Service

11.44 The voluntary jurisdiction covers complaints that are beyond the scope of the compulsory jurisdiction. It is available to payment service providers, e-money issuers, and other financial businesses that carry on business outside the UK and want to give their consumers alternative dispute resolution by the Financial Ombudsman Service.

11.45 Firms, payment service providers, and e-money issuers can join the voluntary jurisdiction to allow consumers to take complaints to the Financial Ombudsman Service about acts or omissions before they joined the compulsory jurisdiction.

11.46 Firms that want to join the voluntary jurisdiction should contact the Financial Ombudsman Service (see **Annex 2 – Useful Contact Details**).

Complaints to the FCA

11.47 We are required to maintain arrangements to enable payment service users, e-money holders and other interested parties (including consumer associations) to submit

complaints to us about payment service providers' or e-money issuers' alleged breaches of the PSRs 2017 or EMRs. Information about how to complain can be found on our website.

11.48 Our process for dealing with these complaints takes account of the Guidelines on Procedures for Complaints of Alleged Infringements of Directive (EU) 2015/2366 issued by the EBA under Article 100(6) PSD2[18]

11.49 These complaints will be acknowledged and used, where appropriate, to inform our regulatory activities — see **Chapter 12 - Supervision**. We do not operate a redress mechanism for individual complaints and so in replying to complainants, we will tell them – where appropriate – that they may be able to refer their complaint to the Financial Ombudsman Service.

Complaints about the FCA

11.50 Anyone directly affected by the way in which the FCA has exercised its functions (other than its legislative functions) may lodge a complaint. To do so, please contact the Complaints Team by email or by telephone on 020 7066 9870.

[18] https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-procedures-for-complaints-of-alleged-infringements-of-the-psd2

12. Supervision

12.1 This chapter describes how we supervise PSPs and e-money issuers under the PSRs 2017 and EMRs 2011. We also summarise our supervisory approach under the Money Laundering and Transfer of Funds (Information on the Payer) Regulations 2017.

Introduction

12.2 All PSPs and e-money issuers will be supervised in accordance with the FCA's general approach to supervision.[19] The specific supervisory measures that we decide to use will depend on the risk posed by an individual business; a category of business or by the sector as a whole.

12.3 Our preference is to work in an open and cooperative relationship with PSPs and e-money issuers. We encourage PSPs and e-money issuers to speak to us at the earliest opportunity if they anticipate any challenges to their compliance with the PSRs 2017 or the EMRs so that we can discuss an appropriate way forward with them. PSPs and e-money issuers should note the ongoing requirement to tell us of any significant changes to their business or conditions of authorisation or registration.[20]

12.4 We may instigate a closer supervisory relationship with any PSP or e-money issuer whose market activity means that any shortcomings or compliance failures could pose a greater risk.

12.5 We may also classify a PI or an EMI with a significant market presence as a "fixed portfolio firm". Fixed portfolio firms are subject to the highest level of supervisory attention. We make it clear to a PI or EMI if it falls within the 'fixed portfolio' category.

Supervising compliance

12.6 We are responsible for supervising PSPs' and e-money issuers' compliance with the following key areas:

- the conduct of business rules under the EMRs and PSRs 2017 (as set out in **Chapter 8 – Conduct of business requirements**);
- authorisation and registration requirements for PIs, RAISPs, and EMIs, which includes initial and ongoing capital requirements, safeguarding and the appointment and registration of agents; and
- (for businesses that are supervised by us for these purposes) money laundering and counter terrorist financing obligations.

12.7 We supervise and monitor compliance with the PSRs 2017 and EMRs through a combination of:

---

[19] Details of which can be found at https://www.fca.org.uk/about/supervision.

[20] See regulation 37 PSRs 2017, regulation 37 EMRs and Chapter 4 of the Approach Document (Change in circumstances of authorisation)

- periodic reporting;
- event driven notifications;
- complaints and other intelligence;
- targeted information gathering and investigations using our statutory powers;
- reporting from auditors; and
- thematic reviews.

12.8 The information we receive (e.g. from reports and notifications) is analysed and further supervisory action may be considered where, for example, the PSRs 2017 requirements are breached. It is likely in such circumstances that we will ask the PSP or e-money issuer for an explanation of why it breached the relevant requirements and then agree remedial action. If we are not satisfied with the response, we will consider enforcement action, including cancelling its authorisation or registration.

12.9 Further details of the reporting and notification requirements can be found in **Chapter 13 – Reporting and notifications** and **Chapter 4 – Changes in circumstances of authorisation.**

12.10 We also monitor compliance through intelligence received via complaints, whistle-blowers and market developments. This approach helps us to identify risks in ongoing compliance. Complaints or other information we receive about breaches of the conduct of business rules are an indicator of whether a PSP or e-money issuer is maintaining appropriate arrangements in relation to governance, systems and controls, and internal controls. Our process for dealing with complaints about alleged breaches of the PSRs 2017 takes into consideration the EBA Guidelines on Procedures for Complaints of Alleged Infringements of Directive (EU) 2015/2366 [to be issued under Article 100(6) PSD2 following consultation].[21]

12.11 Where themes arise from the analysis of information obtained by us that indicate an industry-wide problem, we may undertake supervisory action relating to that theme, such as visiting PSPs or e-money issuers to understand how they are managing the risk(s) identified. Findings from these visits may lead to specific action being required by certain PSPs or e-money issuers and wider guidance being given to the industry.

12.12 PSPs and e-money issuers should be aware that they are "relevant firms" for the purposes of section 404 of FSMA (Consumer redress schemes). Section 404 allows the FCA in certain specified circumstances relating to regular or systemic non-compliance with applicable requirements to make rules requiring relevant firms to establish and operate a consumer redress scheme. More information on consumer redress schemes can be found in Guidance Note 10[22].

Supervision of passporting EMIs and PIs

12.13 We are responsible for supervising compliance with the conduct of business requirements and, where relevant, anti-money laundering and counter-terrorist

[21] https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-procedures-for-complaints-of-alleged-infringements-of-the-psd2

[22] https://www.fca.org.uk/publication/guidance-consultation/guidance10.pdf

financing requirements of EEA authorised EMIs and PIs in relation to services provided from an establishment in the UK. Please refer to **Chapter 6 — Passporting** for further details.

12.14 Where a PI's or EMI's head office is situated in another Member State and operates in the UK through agents pursuant to the right of establishment, that PI or EMI may be required to appoint a central contact point in the UK in order to facilitate the supervision of those network of agents. [The circumstances in which the appointment of a central contact point is appropriate and the functions of the contract point shall be determined in accordance with the Regulatory Technical Standards developed by the EBA under Art 29(5) of PSD2. We will, where necessary, update our approach in respect of the appointment of central contact points following publication of the relevant Regulatory Technical Standards in the Official Journal.]

12.15 Under the PSRs 2017 and the EMRs we may direct that an EEA authorised PI or EMI providing payment services through a branch or agent in the UK reports to us on its regulated activities for information and statistical purposes and (where the EEA authorised PI or EMI has exercised its right of establishment in the UK) to monitor compliance with Parts 6 and 7 of the PSRs 2017. [The EBA is developing Regulatory Technical Standards under Article 29(6) of PSD2 that specify the means, details and frequency of reporting requested by host Member States. We will, where necessary, update our approach in respect of the reporting requirements following publication of the relevant Regulatory Technical Standards in the Official Journal.]

Powers to require information, appoint persons to carry out investigations and carry out skilled persons reports

12.16 We have a number of statutory powers that enable us to obtain information from PSPs and e-money issuers for supervisory purposes. They include:

- the power to require specified information in connection with our responsibilities under the PSRs 2017 and EMRs
- the power to require a report from a skilled person, nominated or approved by us, on any matter that we require in connection with our responsibilities under the PSRs 2017 and EMRs. Further information on our policy on the use of skilled persons and appointment and reporting process is contained in the supervision section of our Handbook (SUP), specifically at SUP 5.3 and 5.4.
- if there is a good reason for doing so, we can appoint competent persons to conduct an investigation on our behalf

12.17 Where, following any investigation, we are not satisfied that a PSP or e-money issuer has dealt appropriately with the causes of the non-compliance, we will discuss the matter with our Enforcement division. **Chapter 14 - Enforcement** contains further details on our approach to enforcement.

Information from auditors

12.18 Statutory auditors and audit firms are obliged under the PSRs 2017 and EMRs to report to the FCA certain matters of which they have become aware in their capacity

as auditor of an authorised PI, an EMI or a person with close links[23] to the authorised PI or EMI. If, for example, an auditor of an authorised PI reasonably believes that the authorised PI has contravened any of the requirements of the PSRs 2017, they must report the contravention to us under regulation 24 of the PSRs 2017 (there is an equivalent obligation on auditors under regulation 25 of the EMRs).

12.19 We will review any information received from auditors and will follow up with the PSP or e-money issuer and/or the auditors as appropriate.

Credit institutions and other FSMA-regulated firms

12.20 Credit institutions and other FSMA-regulated firms that issue e-money or provide payment services are supervised for compliance with the applicable conduct of business rules found in the PSRs 2017 and EMRs in the manner set out in this Chapter.

Group Supervision

12.21 The approach taken for the supervision of a PI or EMI that is part of a large FSMA-authorised group is determined on a case-by-case basis.

Supervision under the Money Laundering and Transfer of Funds (Information on the Payer) Regulations 2017

12.22 The Money Laundering and Transfer of Funds (Information on the Payer) Regulations 2017 (the "MLRs") apply to all PSPs and e-money issuers. [Please note the MLRs were recently subject to consultation and final regulations have not been published by HM Treasury].

12.23 PSPs and e-money issuers must also note their obligations under the Terrorism Act 2000, the Proceeds of Crime Act 2002 and, where relevant, any requirements imposed by the Treasury under the Counter-Terrorism Act 2008. **Chapter 19 – Financial Crime** contains further detail on our approach to financial crime.

12.24 The FCA is the designated supervisory authority under the MLRs for the following types of PSP and e-money issuer:

- credit institutions and other FSMA-regulated financial institutions other than "excluded money service businesses"[24];
- EMIs;
- PIs other than those that have authorisation to provide money remittance payment services (see below); and
- RAISPs.

[23] 'Close links' has a specific meaning in this context. Please refer to regulation 25 of the EMRs and regulation 24 of the PSRs.

[24] An 'excluded money service business' is a money service business with permission under FSMA relating to or connected with credit agreements and contracts for hire of goods but does not have permission to carry on any other kind of regulated activity (see regulation 7 of the MLRs).

12.25 PIs, including "bill payment service providers"[25], that are authorised to provide money remittance services[26] only, are supervised for compliance with the MLRs by HMRC and need to register with HMRC accordingly[27]. PIs (including bill payment service providers) with permission to carry on money remittance plus other, additional payment services may be supervised under the MLRs by either of the FCA or HMRC, depending on the nature of the regulated payment services activity carried out. In these cases, the FCA and HMRC will consider the business activities and scope of the authorisation on a case-by-case basis to determine which supervisory authority is best placed to supervise the PI's compliance with the MLRs.

12.26 There is no need for PIs or EMIs supervised by the FCA under the MLRs to register separately as an Annex I Financial Institution. If you are currently registered with the FCA as an Annex 1 Financial Institution you can apply to us to deregister to avoid additional fees.

12.27 The FCA has a risk-based approach to financial crime supervision. You can find more details about our approach to Anti-Money laundering (AML) supervision in our annual AML reports. Firms that we supervise should be prepared to provide us on request with information about the operation and effectiveness of their AML and counter-terrorist financing policies and procedures that they are required to have in place under regulation 19(1) to (5) of the new MLRs. We may include any PI or EMI in our thematic reviews.

12.28 All firms that the FCA supervises can find helpful guidance on how to prevent financial crime in the FCA's Financial Crime: A Guide for Firms.

[25] As defined in regulation 3(1) of the MLRs
[26] The activity listed at paragraph 1(f) of Part 1, Schedule 1 of the PSRs 2017
[27] See the information for money service businesses on the gov.uk website: https://www.gov.uk/guidance/money-laundering-regulations-money-service-business-registration

13. Reporting and notifications

13.1 PSPs, electronic money issuers and other businesses are required under the PSRs 2017 and the EMRs to provide certain data and information to the FCA either periodically or under specified circumstances. In some cases we must provide this information in turn to the Treasury, European Commission, European Banking Authority (EBA) or European Central Bank (ECB).

13.2 Chapter 4 - Changes in circumstances of authorisation or registration covers the notifications that PIs, EMIs and RAISPs must provide to us when there is (or is likely to be) a significant change in circumstances which is relevant to their authorisation or the information previously provided to us. This includes, for example, changes to standing data, control of the business, outsourcing arrangements and the people responsible for management. Chapter 4 also covers the notice requirements that apply to the persons proposing to increase or reduce their control of the authorised PI, or EMI.

13.3 This chapter deals with the periodic reports that are required under the PSRs 2017 and EMRs and the event-driven notification requirements under the PSRs 2017. It also covers the notifications that are required from "excluded providers" under regulations 38 (Notification of use of limited network exclusion) and 39 (Notification of use of electronic communications exclusion) of the PSRs 2017.

13.4 This chapter is therefore relevant to PSPs, e-money issuers and excluded providers.

Regular reporting

13.5 A summary of the regular reporting requirements for PSPs and e-money issuers is shown in the tables below.

Report required – FSA056 **(**Authorised Payment Institution Capital Adequacy Return)
Required to submit: Authorised PIs and RAISPs **Frequency:** Annual. **Submission date**: Within 30 business days of the authorised PI's or RAISP's accounting reference date. **Method of submission:** Gabriel **Handbook references:** SUP 16.13 (Reporting under the Payment Services Regulations), SUP 16 Annex 27AD (Authorised Payment Institution Capital Adequacy Return), SUP Annex 27B (Notes on Completing FSA056)

Content and purpose

The information requested in this report helps us discharge our supervisory functions by providing us with information on the authorised PI's or RAISP's business and whether it meets its authorization and prudential requirements. The authorised PI or RAISP will only be expected to answer the questions that are relevant to the regulated activities it carries out. For example, RAISPs will need to provide information on the value and volume of the AIS activity, but are not expected to answer the questions on capital resources, safeguarding or payment transactions.

In this report, the authorised PI is asked to provide the following information:

- whether it is included in the consolidated supervision of a parent credit institution (to allow us to supervise groups efficiently)
- a high level income statement covering regulated payment services and non-regulated activities (to give us an overview of the size of the payment services business)
- its capital requirement calculation and details of its capital resources (to determine whether the capital requirement is appropriately calculated and whether it is being met)
- details of its safeguarding methods (to confirm that appropriate arrangements are in place)
- the number of agents appointed (to verify the information on our public register on our website)
- how it accesses payment systems (to help us understand the wider payments infrastructure that it relies on)
- the volume and value of payment transactions executed (including through agents) and the number of payment services customers (to understand the scale of the payment services activity)
- where relevant, information on the volume of AIS or PIS activity, the calculated minimum monetary amount of the professional indemnity insurance and whether the terms of the insurance policy held has changed in any material way since authorisation (to assess the continued suitability of the insurance cover)

RAISPs are asked to provide the following information:

- a high level income statement covering regulated payment services and non-regulated activities (to give us an overview of the size of the payment services business)
- information on the volume of AIS activity, the calculated minimum monetary amount of the professional indemnity insurance and whether the terms of the insurance policy held have changed in any material way since authorisation (to assess the continued suitability of the insurance cover)

Process

Authorised PIs and RAISPs should follow the instructions on the Gabriel online system to submit their returns electronically. Gabriel can also be used to view a tailored schedule of your reporting requirements.

Report required**:** FSA057 (Payment Services Directive Transactions)
Required to submit: Small PIs **Frequency:** Annual report covering 1 January to 31 December. **Submission date:** To be submitted by the end of the following January. **Method of submission:** [To be confirmed] **Handbook references:** SUP 16.13 (Reporting under the Payment Services Regulations), SUP 16 Annex 28C (Small Payment Institution Return), SUP Annex 28D (Notes on completing FSA057)
Content and purpose
The information requested in this report helps us discharge our supervisory functions by providing us with information on the small PI's business and whether it continues to meet the conditions of its registration. In this report, the small PI is asked to provide the following information: • a high level income statement covering regulated payment services and non-regulated activities (to give us an overview of the size of the payment services business) • the volume and value of payment transactions executed by the small PI, including through its agents in the UK (to enable us to provide the Treasury with the necessary information so that it can report the total value of small PI payment transactions to the Commission and further to assess whether the small PI has continued to meet the conditions for registration) • the number of payment services customers (to understand the scale of the payment services activity) • where voluntarily adopted, the details of its safeguarding methods (to confirm that appropriate arrangements are in place) • the number of agents appointed (to verify the information on our public register on our website) • how it accesses payment systems (to help us understand the wider payments infrastructure that the small PI relies on)
Process
[To be confirmed]

Report required: FIN060 (EMI and SEMI Annual Return)

Required to submit: **A**uthorised and small EMIs

Frequency: Annual.

Submission date: Within 30 business days of the EMI's accounting reference date.

Method of submission: [To be confirmed]

Handbook references: SUP 16.15 (Reporting under the Electronic Money Regulations), SUP 16 Annex 30H (FIN060 EMI Questionnaire), SUP 16 Annex 30I (Notes on completing the authorised electronic money institution questionaire), SUP 16 Annex 30J (FIN060 SEMI Questionnaire), SUP 16 Annex 30K (Notes on completing the small electronic money institution questionnaire).

Content and purpose

The information requested in this report helps us discharge our supervisory functions by providing us with information on the authorised or small EMI's business and (where relevant) whether it meets its prudential requirements.

The information that must be provided depends on whether the business is an authorised EMI or a small EMI.

The authorised EMI is asked to provide the following information:

- a high level income statement covering e-money issuance and, where relevant, unrelated payment services; (to give us an overview of the size of the e-money and unrelated payment services business)
- the amount of e-money outstanding and the number of accounts open the end of the reporting period; (to understand the overall size of the market, the authorised EMI's market share and its growth over the reporting period)
- where relevant, the volume and value of payment transactions carried out that are unrelated to the issuance of e-money (to understand the size of the payment services element of the authorised EMI's business)
- its capital requirement calculation and details of its capital resources (to determine whether the capital requirement is appropriately calculated and whether it is being met)
- details of its safeguarding methods (to confirm that appropriate arrangements are in place)
- the number of agents appointed (to verify the information on our public register on our website)
- how it accesses payment systems (to help us understand the wider payments infrastructure that the EMI relies on)
- where relevant, information on the volume of AIS/PIS activity, the calculated minimum monetary amount of the professional indemnity insurance and whether the terms of the insurance policy have changed in any material way since authorisation (to assess the continued suitability of the insurance cover)

The small EMI is asked to provide the following information:

- a high level income statement covering e-money issuance and, where relevant, unrelated payment services (to give us an overview of the size of the e-money and unrelated payment services business)
- the amount of e-money outstanding and the number of accounts open at the end of the reporting period (to understand the overall size of the market, the small EMI's market share and its growth over the reporting period)
- where relevant, the volume and value of payment transactions carried out that are unrelated to the issuance of e-money (to understand the size of the payment services element of the small EMI's business)
- the average outstanding e-money as at the end of the reporting period and whether the small EMI has continued to meet the conditions of registration as a small EMI relating to the limits on the average monthly value of e-money and unrelated payment services
- whether the small EMI has generated average outstanding e-money of €500,000 or more during the reporting period (to determine whether the capital requirements apply)
- (where applicable) its capital requirement calculation and details of its capital resources (to determine whether the capital requirement is appropriately calculated and whether it is being met)
- details of its safeguarding methods (to confirm that appropriate arrangements are in place);
- the number of agents appointed (to verify the information on our **public register on our website**)

how it accesses payment systems (to help us understand the wider payments infrastructure that the small EMI relies on)

Process

[To be confirmed]

Report required: FSA065 Total outstanding e-money at 31 Dec

Businesses required to submit: Small EMIs

Frequency: Annual

Submission date: Within 1 month of the reporting end date (the reporting period runs from 1 January – 31 December)

Method of submission: Email

Handbook references: SUP 16.15 (Reporting under the Electronic Money Regulations) and Sup 16 Annex 30G (SEMI total outstanding e-money return).

Content and purpose

Every year the Treasury must inform the European Commission of the number of natural and legal persons that are registered with us as small EMIs and provide an aggregated e-money outstanding figure for the entire small EMI population. We must report the position as at 31 December in each calendar year. This report is required for the FCA to meet its obligation in providing the requisite information to the Treasury.

Process

FSA065 is available on our website and at SUP 16 Annex 30G. The form should be completed and provided by email to regulatory.reports@fca.org.uk.

Report required: Average outstanding e-money

Required to submit: e-money issuers that are not credit institutions or EMIs, which under the EMRs, includes: the Post Office Limited, the Bank of England, the ECB and the national central banks of EEA States other than the United Kingdom when not acting in their capacity as a monetary authority or other public authority, government departments and local authorities when acting in their capacity as public authorities, credit unions, municipal banks and the National Savings Bank

Frequency: Annual

Submission date: Within 1 month of the reporting end date (the reporting period runs from 1 January – 31 December)

Method of submission: e-mail

Handbook references: SUP 16.15 (Reporting under the Electronic Money Regulations)

Content and purpose

If any of the entities permitted to issue e-money under regulation 63 of the EMRs (that are not credit institutions, EMIs or EEA authorised EMIs) begin to issue e-money in the UK, they will have to report their average outstanding e-money on a yearly basis so we can have more complete information on the size of the e-money market.

Process

The information should be provided by email to regulatory.reports@fca.org.uk

Report required – DISP 1 Annex 1AD Payment Services and electronic money complaints report
Required to submit: All PSPs (Credit institutions, PIs, and EMIs) **Frequency:** Annual **Submission date:** Within 30 business days of firm's accounting reference date (ARD). If the firm does not have an accounting reference date, within 30 business days of 31 December. Please note, The first relevant reporting period following 13 January 2018 is different – see DISP 1.10B. **Method of submission:** [To be confirmed] **Handbook references:** DISP 1.10B (Payment services and electronic money complaints reporting), DISP 1 Annex 1AD (the electronic money and payment services complaints return form)
Content and purpose
To enable us to monitor complaints received by payment service users, including persons who are eligible to complain to the Financial Ombudsman Service about the provision of payment services across the payment services market and to monitor compliance with DISP 1 and regulation 101 of the PSRs.
Process
[To be confirmed]

Report required – REP017 Payments Fraud Report
Required to submit: All PSPs (Credit institutions, PIs EMIs, RAISPs and other PSPs) **Frequency:** Annual **Submission date:** Within 1 month of the reporting end date (the reporting period runs from 1 January – 31 December) **Method of submission: [To be confirmed]** **Handbook references:** SUP 16.13 (Reporting under the Payment services Regulations), SUP 16 Annex 27E (REP017 Payments Fraud Report), SUP 16 Annex 27F (Notes on completing REP017 Payments Fraud Report).
Content and purpose

PSPs are required to provide us, at least annually, with statistical data on fraud relating to different means of payment under regulation 109(4) of the PSRs 2017. We are required in turn to provide these data to the EBA and ECB in aggregated form.

This information will help us understand whether PSPs have appropriate systems and controls to adequately protect users against fraud and financial crime and to understand the security risks faced by the industry as a whole.

Process

[To be confirmed]

Reports required – REP002 Annual controllers report and REP001 annual close links report

Required to submit: authorised EMIs and authorised PIs. Note that credit institutions and other FSMA–regulated firms have an equivalent obligation under SUP 16.4 and SUP 16.5.

Frequency: Annual

Submission date: Within 4 months of the institution's accounting reference date.

Method of submission: [To be confirmed]

Handbook references: SUP 16.15.5 D (for authorised EMIs) and SUP 16.13.3-A D (for authorised PIs).

Content and purpose

Controllers report

Under the EMRs and the PSRs 2017, persons acquiring or disposing of a qualifying holding in the relevant institution must seek our approval for the change in control. We expect authorised PIs and authorised EMIs to understand who owns their business and, in accordance with regulation 37 of the EMRs and PSRs 2017, notify us of any change in circumstance.

The controllers report asks for information on the current control structure and will allow us to verify that the authorised PIs and authorised EMIs as well as the persons that control them, are providing us with the appropriate information in accordance with their obligations.

Close links report

If an authorised PI or authorised EMI has close links, then we must be satisfied that those links are not likely to prevent our effective supervision of the relevant institution. In the close links report the institution is asked to provide information on its close links (including a group organisation chart) and to confirm whether there have been any material changes to the institution's close links since the submission of the last report (or application for authorisation). The information provided will allow us to confirm the relevant institution's ongoing compliance with its conditions of authorisation.

Process

[To be confirmed].

Report required – REP-CRIM Annual financial crime report

Required to submit: EMIs that have reported total revenue of £5 million or more as at its last accounting reference date. Note that credit institutions and other FSMA–regulated firms have an equivalent obligation under SUP 16.23.

Frequency: Annual

Submission date: Within 60 business days of the EMI's accounting reference date.

Method of submission: [To be confirmed]

Handbook references: SUP 16.15.5A

Content and purpose

In this report, the EMI is asked to provide information on:

- the jurisdictions in which it operates
- the number of customers in certain high risk categories customers
- the number of customers in the certain geographical areas
- compliance with financial crime legislation including suspicious activity reports filed
- the number of staff occupying financial crime roles
- sanctions screening
- the top three most prevalent types of fraud

The purpose of this report is to ensure that the FCA receives regular and comprehensive information about the firm's systems and controls in preventing financial crime and to assess the nature of financial crime risks within the industry.

Process

[To be confirmed]

Credit institutions that offer e-money

13.6 Credit institutions that issue e-money are expected to report the amount of their e-money liabilities on a periodic basis. The frequency and form of this reporting will depend on the type of regulated activities undertaken by the credit institution and its group structure. Credit institutions will not be required to complete any additional returns.

Accounting information for payment services and e-money issuance

13.7 Under regulation 24 of the PSRs 2017, authorised PIs that carry on activity other than the provision of payment services are required to provide separate accounting information to the FCA in respect of its provision of payment services. Such information must be subject, where relevant, to an auditor's report. Authorised EMIs that carry on activity other than the issuance of e-money and the provision of payment services have an equivalent obligation under regulation 25 of the EMRs. Information required under regulations 24 PSRs 2017 and 25 of the EMRs should be provided by email to regulatory.reports@fca.org.uk.

Late submission of returns

13.8 PSPs and e-money issuers must comply with the deadlines for sending regulatory data to us. Our normal data collection processes will apply so PSPs and e-money issuers failing to meet the reporting deadlines will be reminded to do so and be subject to an administrative charge of £250. This is in common with reporting by all FCA-authorised or registered firms, which is received and processed in the same way as returns and reports required under the EMRs and PSRs 2017 will be.

Notifications

13.9 A summary of the notification requirements for PSPs and e-money issuers is shown in the tables below.

Notification required – NOT002 Payment Account Service rejections or withdrawals
Required to notify: Credit institutions **When to notify:** A credit institution must submit the notification at the same time as it informs the PSP (as defined in regulation 105) of its refusal of a request for access to payment account services from a PSP[28] **Method of submission:** [To be confirmed] **Handbook reference:** SUP 15.14 (Notifications under the Payment Services Regulations), SUP 15 Annex 9 (Form NOT002 Payment Account Service rejections or withdrawals)
Content and purpose
Under regulation 105(3), a credit institution that refuses a PSP's request to access payment account services must provide duly motivated reasons for the refusal to the FCA. We will use the information provided in this notification for the purposes of supervising compliance with regulation 105 (jointly with the PSR). Please refer to Chapter 16 - Access to payment account services for more information.
Process [To be confirmed]

[28] If, for any reason the credit institution does not notify the PSP of its refusal, it must submit the notification immediately following its decision to refuse access.

Notification required –NOT003 AIS/PIS denial
Required to notify: account servicing payment service providers (ASPSPs) **When to notify:** The ASPSP must notify the FCA immediately if it denies an AISP/PISP access to a payment account and subsequently if and when access is restored. **Method of submission:** [To be confirmed] **Handbook reference:** SUP 15.14 (Notifications under the Payment Services Regulations), SUP 15 Annex 10 (Form NOT003 AIS/PIS denial).
Content and purpose
Under regulation 71(8)(c), an ASPSP that denies a PISP or AISP access to a payment account must submit a notification to the FCA. The notification must include the details of the case and the reasons for taking action. Please refer to Chapter 17 – Payment initiation and account information services and confirmation of availability of funds for more information.
Process [To be confirmed]

Notification required – Credit institutions providing (or intending to provide) account information or payment initiation services
Required to notify: Credit institutions **When to notify:** before the credit institution begins providing such services **Method of submission:** email **Handbook reference:** SUP 15.8.12 D – SUP 15.8.15D and SUP 15.7.1
Content and purpose
The credit institution is required to provide a description of the AIS or PIS activity. We require this information in order to improve our understanding of the providers in this new and emerging market. This will help us measure potential risks to consumers, as well as indicate how competition is working in the sector.
Process Credit institutions should use the form at SUP 14 Annex 4 and return by email to an address for the firm's usual supervisory contact at the FCA.

Notification required – Regulation 38 Notification of services carried out under the limited network exclusion

Required to notify: A provider of services falling within paragraph 2(k)(i) to (iii) of Schedule 1 to the PSRs 2017 (activities involving limited network payment instruments which do not constitute payment services), where total value of the payment transactions executed through such services in any period of 12 months exceeds €1million.

When to notify: The notification must be sent within 28 days of the conditions for notification being met. Further annual notifications will be required thereafter if the conditions for notification continue to be met.

Method of submission: Connect

Further information on how to complete and submit the form can be found on our website.

Content and purpose

This notification is required under regulation 38 of the PSRs 2017. The notification must include a description of the service and the exclusion by virtue of which the services are not payment services. In the notification form we have asked a series of questions designed to illicit sufficient information about the product or service to allow us to determine whether the limited network exemption is applicable. The form of the questions can be found here[29].

For more information on the scope of the limited network exemption please see PERG 15 Q.40.

Process

Businesses should follow the instructions on the Connect online system to submit their notification electronically.

[29] [Link to be provided in final guidance]

Notification required – Regulation 39 Notification of services carried out under the electronic communications network exclusion
Required to notify: A provider (or proposed provider) of services for payment transactions falling within paragraph 2(l) of Schedule 1 to the PSRs 2017 (activities involving electronic communications networks which do not constitute payment services). **When to notify:** Before the service provider begins to provide the relevant services. See the direction on our website for businesses already relying on the exclusion as at 13 Jan 2018. **Method of submission:** Connect Further information on how to complete and submit the form can be found on our website.
Content and purpose
This notification is required under regulation 39 of the PSRs 2017. A person who provides or intends to provide a service falling within the electronic communications networks exemption exclusion must submit to the FCA: (a) a notification including a description of that service; and (b) an annual audit opinion testifying that the transactions for which the services is provided comply with the applicable financial limits. The form of the questions can be found here[30]. For more information on the scope of the electronic communications exemption please see PERG 15 Q41A.
Process Businesses should follow the instructions on the Connect online system to submit their notification and auditor's report electronically.

[30] [Link to be provided in final guidance]

Further planned information in the Approach Document

PSD2 confers mandates on the EBA to develop Regulatory Technical Standards (RTS) and Guidelines to provide further detail on what is required under the certain of the provisions of PSD2. The RTS and Guidelines under development cover a number of reporting and notification requirements for PSPs. We plan to provide guidance or signpost as necessary once the EBA finalises the relevant Guidelines and the Commission publishes the relevant RTS in the Official Journal of the EU.

Reporting and notification requirements likely to be included in this chapter following final EBA Guidelines or RTS include:

- annual assessments of operational and security risks required under PSD2 article 95(2). This is dependent on EBA Guidelines to be developed under article 95(3) on establishment, implementation and monitoring of security measures, including certification processes where relevant
- reporting to host member states from PIs having agents or branches within host member state territories as may be required under PSD2 article 29(2). This is dependent on EBA RTS to be developed under article 29(6)
- Reporting required in accordance with the RTS developed under PSD2 article 98. ASPSPs will be required to report to the competent authority on deficiencies in the dedicated interface for use of AIS or PIS providers. [See final draft RTS article 28(2)b]
- notification of major operational or security incidents as required under PSD2 article 96(1). This is dependent on Guidelines to be developed under article 96(3)

14. Enforcement

14.1 This chapter describes our enforcement approach. It is relevant to PSPs and e-money issuers and other persons who are subject to our enforcement action under the PSRs 2017 and EMRs (including agents and excluded providers[31]).

Our enforcement approach

14.2 Our approach to enforcing the PSRs 2017 and EMRs mirrors our general approach to enforcement under the Financial Services and Markets Act 2000 (FSMA).[32] This is set out in Chapter 2 of the Enforcement Guide (EG).

14.3 We seek to exercise our enforcement powers in a manner that is transparent, proportionate, responsive to the issue and consistent with our publicly stated policies. We also seek to ensure fair treatment when exercising our enforcement powers. Finally, we aim to:

- change the behaviour of the person who is the subject of the action;
- deter future non-compliance by others;
- eliminate any financial gain or benefit from non-compliance; and
- where appropriate, remedy the harm caused by the non-compliance.

14.4 Our approach for selecting cases for formal enforcement action in respect of unauthorised activity covers provision of payment services by persons that are not payment service providers or issuance of e-money by persons that are not e-money issuers and follows our approach set out in EG 2.4.

How cases are referred to the Enforcement division

14.5 When we consider whether to refer a case (whether under FSMA, the PSRs 2017 or EMRs) to the Enforcement division for investigation, we take a number of criteria into account. We have framed the criteria as a set of questions. They take into account our statutory objectives, business priorities and other issues, such as the response of the person to the issues we are considering for referral.

14.6 Not all the criteria will be relevant to every case and there may be other considerations which are not listed below that are relevant to a particular case. Staff from the referring department, the Enforcement division and, in some cases, from other areas of the FCA work together to decide whether to refer a case for investigation. The referral criteria include the following:

- is there actual or potential consumer loss/detriment?
- is there evidence of financial crime or risk of financial crime?

---

[31] Note that the definition of "payment service provider" includes agents of payment service providers and excluded providers for the purposes of Part 9 (the Authority) and Schedule 6 (application and modification of legislation) of the PSRs 2017.

[32] Any breaches of DISP will be enforced using the normal FSMA procedures.

- are there issues that indicate a widespread problem or weakness at the business?
- is there evidence that the business/person has profited from the action or potential breaches?
- has the business failed to bring the actions or potential breaches to our attention?
- what was the reaction of the business/person to the breach?

14.7 The criteria may change from time to time; more information can be found on our website.

What tools will we use when investigating breaches?

14.8 The PSRs 2017 and EMRs allow us to use many of the powers of investigation we have under FSMA. The regulatory powers provided to us by the PSRs 2017 and EMRs include the following:

- Information requirements: we may require information by serving written notice on any person.
- Interviews: we may require individuals connected to the PSP or e-money issuer or connected to the investigation to attend an interview and answer questions.
- Search warrants: we may apply to the court for a search warrant to allow for the entry and searching of premises and the obtaining of documents.

Sanctions for breaches of the PSRs 2017 and EMRs

14.9 The PSRs 2017 and EMRs allow us to impose penalties and censures for breaches of their requirements, and to instigate criminal prosecutions, including against those persons who provide or claim to provide payment services or who provide or claim to issue e-money but are not authorised or registered to do so (or are otherwise exempt). We can also order PSPs or e-money issuers, agents and excluded providers to provide restitution to their customers.

14.10 We can cancel, vary or place requirements on a PI's, RAISP's or EMI's authorisation or registration where certain criteria, outlined in the PSRs 2017 and EMRs, are met. In addition to serious breaches of the PSRs 2017 and EMRs, examples of the circumstances where we may cancel an authorisation or registration include, but are not limited to, persistent non-payment of fees and levies owed to us, non-submission of an annual return and failing to provide us with current contact information.

14.11 We have an additional power under regulation 52 of the EMRs that allows us to suspend an EMI's authorisation or registration (as applicable) or impose limitations or other restrictions on its payment services or e-money business activities for a maximum of 12 months as we consider appropriate.

14.12 When we inform an EMI that we are taking such action, we will include details of the period for which the suspension, limitation or restriction of activity may apply.

14.13 Our policy in relation to how we impose penalties on PSPs and e-money issuers and other persons who breach our rules or the requirements of the PSRs 2017 and EMRs

can be found in Chapter 19 of our Enforcement Guide (EG), where we explain that we will have regard to Chapter 6 of our Decision Procedure and Penalties Manual (DEPP).

14.14 We will have regard to the relevant factors in DEPP 6.2 in deciding whether to take action or not, and DEPP 6.4 in deciding whether such action should be a financial penalty. If we decide that a financial penalty is appropriate, we will have regard to DEPP 6.5 – 6.5D, which sets out the factors we will take into account in setting the level of penalty.

14.15 Under the PSRs 2017, we also have enforcement powers over EEA authorised PIs, EEA authorised EMIs and EEA RAISPs. We can take precautionary measures pending action by the home Member State competent authority (i.e. the competent authority where the authorised PI, authorised EMI or RAISP is authorised or registered) where immediate action is necessary to address a serious risk to the collective interest of customers in the UK. We will withdraw the temporary measures when the risk has been addressed.

The process when imposing penalties or censures

14.16 Before imposing a penalty, we will inform the person or business that we intend to do so. We will also tell them the reasons for imposing a penalty or censure and, where relevant, its amount. They will have at least 28 days to make representations to us, should they wish to do so. After this, we will make a decision whether or not to take action. If we decide to proceed, and if the decision is contested, there is a right to refer the matter to the Upper Tribunal (Financial Services), which is an independent judicial body. As with cases under FSMA, we may settle or mediate appropriate cases involving civil breaches of the PSRs 2017 and EMRs. Both DEPP 6.7 and EG 5 contain further information on our settlement process and settlement discount scheme.

14.17 We may publish enforcement information about a person or business on the Financial Services Register if we consider it appropriate to do so.

Removal of agents from the Financial Services Register

14.18 The PSRs 2017 and EMRs allow us to remove an agent of a PI or EMI from the Financial Services Register in specified circumstances, which include the following:

- where we are not satisfied that the directors and persons responsible for the management of the agent are fit and proper persons;
- the removal is desirable to protect the interests of consumers; or
- if the agent's provision of payment services is otherwise unlawful.

14.19 If we propose to remove an agent from the Financial Services Register other than at the request of the PI or EMI, we will inform the PI or EMI that we intend to do so and give them a warning notice that sets out our reasons for the proposed removal and specifies the period in which the PI or EMI can make representations for us to consider. After this, we will make our decision on whether or not to take the proposed action.

14.20 If we decide to proceed, and the decision is contested, the PI or EMI can refer the matter to the Upper Tribunal (Tax and Chancery Chamber). If the matter is not referred to the Tribunal within 28 days we will remove the agent from the Financial Services Register.

14.21 If the warning notice identifies another person (a third party) and, in our opinion, is prejudicial to that person then section 393 of FSMA (third party rights) applies. We will also give a copy of that notice to the third party, and they also have the right to make representations and refer the notice to the Tribunal if we decide to proceed and take the proposed action[33].

Where can I find more information?

14.22 EG 19 sets out more detail on the use of the FCA's non-FSMA enforcement powers (for example in relation to the PSRs 2017, and the EMRs and the MLRs). Annexes 1 and 2 of Chapter 2 of DEPP set out who will make the decisions to use our disciplinary and enforcement powers under the EMRs and PSRs 2017. Our website also includes further details.

[33] Third party rights also apply to proposed action to cancel an authorisation, registration, to take disciplinary measures or to require restitution.

15. Fees

This year's consultation paper on fee rates (not yet published), will cover regular fee updates as well as proposed amendments to fee structures, necessitated by PSD2. Updated information about fees will be added to this chapter once the fees consultation concludes.

16. Access to payment account services

16.1 Both the FCA and the Payment Systems Regulator are responsible for monitoring compliance with regulation 105 of the PSRs 2017. In this chapter, unless stated otherwise, references to 'we' or 'us' mean the FCA and the Payment Systems Regulator together.

16.2 This chapter sets out the FCA's and Payment Systems Regulator's guidance on how we will apply the provisions of regulation 105, which deals with PSPs' access to payment account services. It is relevant to credit institutions that provide such services and PSPs and prospective PSPs who wish to access these services in order to provide their own payment services. For the purposes of Regulation 105 and this chapter, "PSPs" means:

- authorised PIs
- small PIs
- RAISPs
- EEA authorised PIs
- EEA RAISPs
- EMIs.

16.3 Regulation 105 does not cover the provision of payment account services to other credit institutions or other types of PSP not listed above.

16.4 The regulation also covers a person who has made an application to the FCA or the relevant competent authority in its home EEA State, to be authorised or registered as any of the PSPs listed above. References to PSPs in this chapter include prospective PSPs in this category.

16.5 In line with HM Treasury's interpretation (put forward as part of its consultation on the implementation of PSD2) we consider 'payment account services' provided by credit institutions to include the provision of payment accounts used for the purposes of making payment transactions on behalf of clients, safeguarding accounts and operational accounts. As per regulation 105(2) access to these services must be sufficiently extensive to allow the PSP to provide payment services to its own customers in an unhindered and efficient manner.

The requirements of regulation 105

16.6 Regulation 105 requires that credit institutions must grant PSPs with access to payment account services on a proportionate, objective and non-discriminatory (POND) basis. The regulation also requires credit institutions to:

- provide PSPs which enquire about access to payment account services with the criteria the credit institution applies when considering requests for such access;

- maintain arrangements to ensure those criteria are applied in a manner which ensures that access to payment account services is granted on a POND basis;
- ensure that, where access is provided, it is sufficiently extensive to allow the PSP to provide payment services in an unhindered and efficient manner; and
- notify the FCA of the reasons where access is refused or withdrawn.

16.7 We provide guidance on each of these requirements below.

Granting PSPs access to payment account services on a POND basis

HM Treasury states in its consultation paper that 'the regulation does not impose an absolute obligation for credit institutions to grant access. The decision to work with a given PI is still a commercial one, with credit institutions able to take into account cost and risk.'

16.8 We agree with this statement. In our view, the effect of regulation 105 is to ensure that a credit institution that provides payment account services should consider applications from PSPs individually and on their own merits. It should not have blanket policies restricting access to those services for broad categories of PSPs, without considering the specific risks posed by the business and ways in which a PSP might mitigate the risks.

16.9 This approach means that credit institutions should not deal generically with whole categories of customers or potential customers. Instead, we expect credit institutions to recognise that the costs, risks and potential revenues associated with different business relationships in a single broad category will vary, and to manage those differences appropriately. Regulation 105 reinforces the need to determine applications for banking services by PSPs not simply by reference to membership of a particular category of business, but taking account of the individual circumstances of the specific applicant. This aligns with the expectations the FCA has set out for an effective risk-based approach to managing money-laundering risk by credit institutions.

16.10 A non-exhaustive list of the factors we may consider when assessing whether a credit institution is granting access on a POND basis includes the following (not all of which will necessarily be relevant to all cases):

- Has the credit institution considered the applicant's individual circumstances, including the specific costs, risks and revenues it may present?
- Has the credit institution applied the same criteria or offered the applicant similar terms and conditions to other PSPs that engage in comparable transactions or have a similar profile, taking risk considerations into account (in other words, is it acting in a non-discriminatory way)? We may ask the credit institution to explain any differences.
- Can the credit institution objectively justify a decision not to grant access? If a credit institution has not given a sound justification for its decision, we may require it to provide further reasons. See section 16.36 below on "Providing duly motivated reasons to the FCA"
- Is the credit institution's decision not to grant access to an applicant proportionate? We may assess whether the criteria applied by the credit

institution to the individual applicant, or the information and evidence required to support the application, go beyond what is reasonably necessary to identify and address any concerns the credit institution might have in relation to granting the PSP access.
- Could the credit institution's concerns be addressed in a way that is less onerous than refusing or withdrawing access, but equally effective (for example, by charging a higher price or requiring additional reporting as opposed to restricting access entirely)?

16.11 Factors relating to the process by which the decision was reached will also be relevant to our assessment, for example:

- Has the credit institution provided an opportunity to discuss the application and/or the criteria meaningfully and constructively with the applicant? Has the applicant been given a meaningful opportunity to address any concerns the credit institution may have?
- Has the applicant responded to any requests for information or evidence from the credit institution within appropriate timescales? Has the applicant taken concrete and timely steps to address the credit institution's concerns?

Providing criteria to potential applicants

16.12 When a PSP or prospective PSP is seeking access to payment account services for the purpose of providing payment services (referred to here as a "potential applicant"), it is important that credit institutions are transparent about the requirements the potential applicant will need to meet in order to be granted access i.e. the credit institution's 'criteria'. Regulation 105 requires credit institutions to provide these criteria in response to access enquiries from potential applicants.

16.13 As a preliminary point, we would generally expect credit institutions to clearly signpost the channels through which potential applicants can make enquiries about access to payment account services (for example, a dedicated email address or telephone line). Through these channels information should be readily available about the payment account services offered by the credit institution, how to apply and the estimated timeframe for decisions to be made on applications.

16.14 Where enquiries are made, credit institutions should provide their criteria to the potential applicant in written form, or, where it is made publicly available, for example on a website, direct the enquiring party to the relevant information.

16.15 The information credit institutions provide should be clear and sufficiently comprehensive so that an applicant could reasonably understand what they are expected to do when making an application. However, this does not extend to disclosing commercially sensitive information about the credit institution's business strategies or risk appetites.

16.16 We would expect credit institutions to be able to objectively justify and explain how the criteria, including any minimum eligibility requirements or exclusions, provided to the potential applicant are necessary to achieve the credit institution's objectives and

to address the risks it has to mitigate, i.e. we would expect the criteria to be based on POND principles.

16.17 As a minimum, we would expect the information provided to the potential applicant to cover all areas against which the credit institution will assess the applicant and its business. For example, this could include setting out for the potential applicant:

- information about the payment account services the credit institution offers;
- any exclusions or minimum eligibility requirements that must be met; or
- the information and evidence the credit institution will require from the potential applicant in support of the application in order to make a decision whether or not to provide payment account services.

16.18 We would also expect credit institutions to keep their criteria under review and update them from time to time in light of experience.

Maintaining arrangements to ensure criteria are applied on a POND basis

16.19 Credit institutions are required to maintain arrangements to ensure their criteria are applied in a manner which ensures access to payment account services is granted on a POND basis. These arrangements should ensure the consistent application of those criteria in practice to every individual application.

16.20 Such arrangements might cover, for example, how clear accountability for decisions is achieved, how relevant staff are trained and how compliance is monitored internally. However, it will be up to each credit institution to be able to demonstrate it is maintaining appropriate arrangements.

16.21 We would expect credit institutions to maintain a record of these arrangements and the governance for setting and making changes to the criteria or their application.

Granting sufficiently extensive access

16.22 Regulation 105 requires that access to payment account services is sufficiently extensive to allow the PSP to provide payment services in an unhindered and efficient manner.

16.23 In assessing whether credit institutions are meeting this requirement, we will consider whether PSPs are able to access the services that are essential to their business activities. In most cases this is likely to include, as a minimum, a payment account (that can be used to execute transactions on behalf of the PSP's users); a business current account (for holding salaries, working capital etc.) and a safeguarding account. For some PSPs, additional products or services may also be essential to support the PSP's specific business activities (for example the ability to make cash deposits may be essential to a business operating within a cash heavy model). We would also expect the credit institution to grant access to such additional services on a POND basis in accordance with regulation 105 and this chapter.

16.24 Regulation 105 does not require credit institutions to provide types of products and services that they do not already provide. However, we would expect credit

institutions to provide clear information to potential applicants on the products and services that are available (including the terms and conditions that apply) as well as the criteria that the credit institution will apply when deciding whether to grant access to such services.

16.25 Similarly, a credit institution may withdraw certain payment account services (or related services) from a PSP or prospective PSP if it can demonstrate that the decision has been made on a POND basis. If any aspect of the payment account service is withdrawn which prevents or obstructs the PSP or prospective PSP from providing its intended payment services, this should be treated as a withdrawal of access and the FCA should be notified in accordance with regulation 105(3) and the following section.

Notifying the FCA where access is refused or withdrawn

16.26 Regulation 105(3) requires a credit institution to provide the FCA with duly motivated reasons where it (i) refuses a PSP or a prospective PSP's request for access to payment account services or (ii) withdraws such access. Under Regulation 105(3), the FCA will share notifications with the Payment Systems Regulator.

Refusal and withdrawal

16.27 Our view is that a refusal of a request for access would cover a situation where a credit institution refused to grant access following consideration of an application and where the credit institution prevented a potential applicant who wanted to make an application for payment account services from doing so.

16.28 It may be the case that a potential applicant has been provided with the relevant information and criteria by a credit institution and wishes to apply to access payment account services, but has been told it is not eligible to do so or has not been permitted to progress its application in a timely manner. We would regard this as a refusal and expect it to be notified to the FCA with duly motivated reasons for the refusal.

16.29 Similarly, a refusal to grant access following consideration of an application should be notified to the FCA with duly motivated reasons.

16.30 Once a PSP or potential PSP has been granted access to the payment account services it applied for, any withdrawal or cancellation of this access by the credit institution should be notified to the FCA with duly motivated reasons.

When the FCA should be notified of refusal or withdrawal

16.31 Regulation 105(3) requires a credit institution to provide the FCA with duly motivated reasons if it refuses a request for access, or withdraws access to payment account services.

16.32 Under SUP 15.14.6 we require the credit institution to notify the FCA of the reasons at the same time as it informs the applicant of its refusal. If, for any reason the credit institution does not notify the applicant of its refusal, the credit institution must submit the notification to the FCA immediately following the decision to refuse access in

accordance with SUP 15.14.7. This also applies in the case of a potential applicant being denied access to the application process, which we treat as a refusal for the purposes of regulation 105(3).

Notifications of withdrawal of access should be made to the FCA at the point that the credit institution gives notice to the PSP or potential PSP that it will terminate the contract for the provision of the whole or part of the payment account services.

Providing duly motivated reasons to the FCA

16.33 In the event of a refusal or withdrawal, a credit institution must submit the notification form **NOT003 AIS/PIS denial**, completed in accordance with the notification rule SUP 15.14.3D.

We will expect "duly motivated reasons" given in the notification to relate specifically to the individual circumstances of the PSP or prospective PSP. We are unlikely to consider blanket or generic statements to constitute 'duly motivated reasons'. For example, where a PSP or prospective PSP falls 'outside a credit institution's commercial appetite,' the credit institution should explain the factors that contributed to this assessment. Where a PSP or potential PSP falls 'outside a credit institution's risk appetite,' the credit institution should explain what elements of the PSP's business present too great a risk.

Monitoring compliance

16.34 The FCA and Payment Systems Regulator must each maintain arrangements designed to enable payment service users and other interested parties to submit complaints to it that a requirement imposed by or under Regulation 105 has been breached by a credit institution. We (the FCA and the Payment Systems Regulator) will consider complaints from individuals which allege infringements of Regulation 105, together with, and in light of, information we receive in notifications under regulation 105(3).

16.35 A decision on whether the Payment Systems Regulator, FCA or both regulators should investigate and take action in relation to potential infringements indicated by notifications, complaints or both, will be made on a case-by-case basis, taking into account the nature of the information received and the roles and responsibilities of each regulator.

16.36 Each regulator in its capacity as competent authority will use its own procedures in order to carry out its duties under the PSRs 2017. For the FCA's procedures and processes as competent authority under the PSRs 2017, please refer to **Chapter 14 - Enforcement.** The Payment Systems Regulator's procedures and processes as competent authority under the PSRs 2017 are included in its draft PSRs 2017 powers and procedures guidance, which can be found at Appendix 1 of its approach document[34].

[34] [See The PSR's proposed approach to monitoring and enforcing the revised Payment Services Directive (PSD2) https://www.psr.org.uk/sites/default/files/media/PDF/Payment-Services-Regs-2017-draft-approach.pdf]

17. Payment initiation and account information services and confirmation of availability of funds

Introduction

17.1 Account information services (AIS) and payment initiation services (PIS) - two services not previously regulated by the FCA - are now in the scope of the PSRs 2017. **Chapter 2 – Scope** and PERG 15 contain further details and examples of the types of services that fall within the description of AIS and PIS.

17.2 The payment service provider providing and maintaining the payment account for the payer is referred to in the PSRs 2017 as the 'account servicing payment service provider' (ASPSP). ASPSPs include businesses that provide 'payment accounts' such as banks, building societies, PIs, e-money issuers and credit card providers.

17.3 The institution providing the account information or payment initiation service is referred to as an 'account information service provider' (AISP) or a 'payment initiation service provider' (PISP). Any institution providing these services is an AISP or PISP whether or not it also provides other payment services under the PSRs 2017 or activities regulated under FSMA. For example, if a credit institution provides PIS or AIS, they will be a PISP or AISP in relation to the provision of that service.

17.4 The PSRs also creates a framework for payment service providers to issue card-based payment instruments which can be used to initiate a payment transaction from an account held by another payment service provider. The institution issuing card-based payment instruments is referred to as a 'card-based payment instrument issuer' (CBPII). Further guidance on this is given in **Chapter 8 – Conduct of business requirements.**

17.5 Also of relevance to ASPSPs, AISPs, PISPs and CBPII's are the Regulatory Technical Standards on strong customer authentication and secure communication (the 'SCA-RTS'). [Once published in the Official Journal of the European Union, the SCA-RTS will become a Commission Delegated Regulation[35]]. The security measures referred to in regulations 68(3)(c), 69(2)(a) and (3)(d), 70(2)(a) and (3)(c) and 100 (secure communication and authentication) and the associated SCA-RTS will apply to firms from 18 months after the SCA-RTS enters into force. The SCA-RTS [once final] should be read alongside the relevant sections in this chapter.

17.6 Having effective control mechanisms in place to manage operational and security risks is a key element of the regime even before the SCA-RTS takes effect. For example, the information that we assess as part of an application for authorisation (or

[35] See https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2/-/regulatory-activity/consultation-paper

re-authorisation) includes a statement of the applicant's security policy, covering a description of the applicant's security control and mitigation measures to provide adequate protection to users and how these measures ensure a high level of technical security and data protection. Regulation 98 of the PSRs 2017 explicitly requires a payment service provider to establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks, relating to the payment services it provides.

17.7 Many other requirements applicable to PISPs and AISPs are set out in **Chapter 8 – Conduct of business requirements**. As authorised PIs, PISPs will be subject to the majority of these requirements and must follow them to the extent that they are applicable to the PISP's business model and the way that the PISP interacts with its customers.

17.8 For AISPs, which Conduct of Business Rules apply will depend on whether they are providing any payment services other than AIS. A business only offering AIS can apply to the FCA to become a RAISP instead of seeking full authorisation. RAISPs are subject to a more limited number of Conduct of Business Rules than other payment service providers. AISPs that are not subject to reduced requirements must follow all of the Conduct of Business Rules to the extent that they are applicable to the AISP's business model and the way that the AISP interacts with its customers.

17.9 This chapter outlines and provides guidance in relation the requirements introduced in the PSRs that relate to AIS and PIS. This chapter is split into five parts:

- scope of accounts subject to the requirements
- requirements on ASPSPs
- requirements on PISPs and AISPs
- requirements on ASPSPs, PISPs and AISPs when communicating and interacting with their customers in relation to these services
- transitional arrangements before the SCA-RTS enter into force

Scope of accounts subject to the requirements

17.10 PERG 15 provides further guidance on the activities that constitute AIS and PIS.

17.11 Regulations 68, 69 and 70 only apply to 'payment accounts' which are 'accessible online'.

17.12 A '**payment account**' means '**an account held in the name of one or more payment service users which is used for the execution of payment transactions**.' We provide guidance on the definition of payment account in PERG 15. Under this guidance, a payment account can include current accounts, e-money accounts, flexible savings accounts, credit card accounts and current account mortgages.

17.13 The meaning of '**accessible online**' is not defined under the PSRs. In our view, an account is accessible online if the ASPSP offers online banking services in relation to that account. Online banking services may be provided through websites or applications, and may be accessible using a desktop computer, mobile phone, tablet or any other such device. An account may be accessible online regardless of whether the

customer has chosen to activate online banking services with the ASPSP. However, the customer may need to activate those services before they can use AIS or PIS, if they do not already have the security credentials for use in the ASPSP's authentication procedures.

17.14 The purposes for which the specific account can be accessed online also need to be considered when determining whether an account is 'accessible online'. Whether regulations 68, 69 and 70 apply to a payment account will partly depend on what the account holding customer could do with that account online. In our view, an account which is available online on a '**view only**' basis, but without any payment functionality, would not be 'accessible online' for the purposes of PIS. It would, however, be 'accessible online' for the purposes of AIS and confirmation of availability of funds to a CBPII.

17.15 The effect of an account being a 'payment account' which is 'accessible online' is that payment service users have a right to use the services of CPBIIs, AISPs and PISPs in relation to these accounts. ASPSPs, CBPIIs, AISPs and PISPs become subject to a number of requirements and we provide guidance on these below.

Requirements on ASPSPs

When requirements on ASPSPs apply (regulations 68(4), 69(2) and 70(2))

17.16 When an ASPSP's customer uses an AIS or gives consent for a payment to be made through a PIS in line with regulation 67, the ASPSP must comply with certain obligations. This consent can be provided directly to the ASPSP or provided via a PISP (e.g. through the use of personalised security credentials) or the payee.

17.17 When an ASPSP's customer has given the ASPSP explicit consent to provide confirmation on availability of funds to a CBPII, the ASPSP must immediately provide such confirmation upon the request of that CBPII.

17.18 Guidance is given at 17.42 below on the meaning of 'explicit consent'.

Communication with CBPIIs, PISPs and AISPs (regulations 68(3)(c) 69(2)(a) and 70(2)(a))

17.19 An ASPSP must communicate with CBPIIs, PISPs and AISPs in accordance with the SCA-RTS once the SCA-RTS apply. In summary, the SCA-RTS will require ASPSPs to offer an interface to AISPs, PISPs and CBPIIs which complies with a number of minimum standards. For example, the interface will need to offer the same level of availability and performance, including support, as well as the same level of contingency measures, as the interface made available to the customer for directly accessing its payment account online and allow AISPs, PISPs and CBPIIs to identify themselves towards ASPSPs.

17.20 In addition, once the SCA-RTS apply ASPSPs will be required to provide the following information to the FCA in respect of the dedicated interface:

- at the request of the FCA - Statistics on the availability and performance of the dedicated interface (RTS Article 28(2)(a))
- where the dedicated interface does not operate at the same level of availability and performance as the interface made available to the account servicing payment service provider's payment service user for accessing its payment account online – a report including the causes of the deficiency and the measures adopted to re-establish the required level of service (RTS Article 28(2)(c))

Confirmation of the availability of funds (regulation 68(4))

17.21 If the ASPSP receives a request that meets the requirements of the SCA-RTS, the ASPSP must immediately provide a yes or no answer on the availability of the amount necessary for the execution of the card-based payment transaction. We consider 'immediately' in this context to mean that the response should be sufficiently fast so as not to cause any material delay in the payment transaction.

Information on the initiation of the payment transaction (regulation 69(2)(b))

17.22 This is only applicable to payment initiation services. As part of the payment initiation process, a PISP will transmit a payment order to the ASPSP for processing. Immediately after receipt of this payment order, the ASPSP must provide or make available to the PISP 'all information on the initiation of the payment transaction and all information accessible to the ASPSP regarding the execution of the payment transaction'. This is likely to take place during the communication session in which the payment is initiated.

17.23 In our view, the requirement to provide or make available 'all information' would include, as a minimum, the information that would be provided or made available to the customer directly if the customer initiated a payment.

Treatment of data requests and payment orders (regulations 69(2)(c) and 70(2)(b))

17.24 ASPSPs must not prohibit or discourage customers from using AIS or PIS (e.g. by communicating to customers that they will be responsible for unauthorised transactions if they share their personalised security credentials with AISPs and PISPs).

17.25 An ASPSP must treat data requests and payment orders from AISPs and PISPs the same as those that come directly from their customer unless it has objective reasons to treat them differently. In our view, the references to "objective reasons" in Article 66 (4) (c) and 67 (3) (b) of PSD2 have the same meaning as in Article 68 (5) PSD2 and only objective and duly evidenced reasons relating to fraudulent or unauthorised access by that AISP or PISP can potentially justify differential treatment.

17.26 For AIS, we expect ASPSPs to make the same information available to a customer via an AISP as would be available to the customer if they accessed their account online directly with the ASPSP. The amount of information which is required to be disclosed will, therefore, differ across ASPSPs and across accounts. To give some examples, we

would expect the following sorts of information to be included where the information is available to the customer directly:

- information relating to the account holder and account, such as the name on the account, address of the account holder, contact details of the account holder and account number; and
- transaction data, which should be provided to the same level of granularity and cover the same time periods as is available to the customer when they access their account directly. However, in our view this does not extend to analysis of any transaction data which an ASPSP provides or makes available to its customers, such as an additional paid for service.

17.27 For payment initiation services, ASPSPs are required to treat the payment order in the same way, in particular in terms of timing, priority or charges, as a payment order initiated by the customer directly.

17.28 We would not expect an ASPSP to treat data requests or payment orders differently on the basis of the cost of processing the request being higher when it is made through a PISP or AISP than when it is made directly by the customer.

17.29 In order to meet this requirement, we expect ASPSPs to allow each customer access via a PISP to the same level of functionality that is available to a customer if they initiate a payment directly with their ASPSP. ASPSPs are not, however, required to provide functionality via a PISP that exceeds the functionality they offer to their customers directly. For example, if an account only has the functionality to initiate payments online to another account in the name of the customer, the ASPSP would not be required to build functionality to allow the customer to initiate payments to a third party via a PISP.

17.30 To give further examples, the following practices would be inconsistent with the requirement to treat data requests and payment orders in the same way as those received from customers:

- processing payments made directly by the customer with the ASPSP as a higher priority than those which are initiated via a PISP;
- limiting the payment types which can be initiated via a PISP (considering the types which can be initiated online directly by the customer);
- sharing less data with AISPs than the customer can directly access online (except where the consumer has not consented to that data being made available or the data are only available to the customer for a fee);
- if an ASPSP charges customers to execute particular transactions, charging different amounts for payments initiated by the customer directly and via a PISP;
- requiring that AISP/PISPs satisfy and evidence particular standards of compliance with legal or regulatory requirements (e.g. data protection or anti-money laundering) in order to gain access to payment accounts;
- imposing different value limits on PISPs in the context of payments schemes (e.g. the faster payments scheme or Bacs) than would be applicable if the customer placed a payment order directly through the ASPSP.

Contractual arrangements (regulations 69(2)(d) and 70(2)(c))

17.31 An ASPSP is prohibited from requiring a PISP or an AISP from entering into a contract with it before complying with its obligations under regulations 69 and 70 and under the SCA-RTS. In our view, this means access should not depend on the AISP or PISP agreeing to any specific arrangements with the ASPSP, for example payment or liability arrangements. Similarly, ASPSPs requiring or suggesting to AISPs or PISPs that a contractual arrangement is required would not be permitted.

17.32 In our view, this does not, however, prohibit the parties from putting contractual arrangements in place if they both wish to do so (provided this is not a pre-condition of access set by the ASPSP). For example, AISPs and/or PISPs may wish to enter into contractual arrangements with an ASPSP for access:

- on more favourable terms than required under the PSRs and the SCA-RTS (for example, entering into a contract to allow a greater frequency of access to the payment account than prescribed in the SCA-RTS); or
- to data or functionality which are not covered by the scope of the PSRs 2017 (e.g. access to information on non-payment accounts).

Denying access to providers of account information services or payment initiation services to payment accounts (regulation 71(7), 71(8))

17.33 An ASPSP may only deny a PISP or AISP access to a payment account for reasonably justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account by that AISP or PISP. This includes the unauthorised or fraudulent initiation of a payment transaction.

17.34 This means access to AISPs and PISPs must not be denied for reasons that do not relate to unauthorised or fraudulent access to the payment account. In our view, an ASPSP may deny access to an AISP or PISP when they suspect, for reasonably justified and duly evidenced reasons, that there has been or will be unauthorised or fraudulent access to the payment account by that AISP or PISP. The fact that a customer is using an AISP or PISP does not by itself give grounds for suspicion of unauthorised or fraudulent activity.

17.35 The regulations and this guidance do not apply to ASPSPs' decisions in relation to access requests to payment account data from businesses that are not authorised or registered providers of AIS or PIS.

17.36 ASPSPs should not deny access to an AISP or PISP solely on the basis that it is a member of a particular category of AISP or PISP. The ASPSP must have an objective justification for, and appropriate evidence to support, a suspicion that fraudulent or unauthorised access by each individual AISP/PISP in that category has occurred or will occur. ASPSPs may, in some circumstances, decide to deny a particular AISP or PISP access only to a specific payment account. However, in our view, in other circumstances an ASPSP may justifiably deny all requests for access to its customers' payment accounts from a particular AISP or PISP while the reasons for that denial of access continue to exist.

17.37 Before denying access the ASPSP must attempt to contact the payment service user, or users to advise them of its intentions and the reason for denying access. If the ASPSP is unable to contact the payment service user(s) beforehand, it must do so immediately after, using the means of communication agreed in the framework contract. However, if providing this information would compromise reasonable security measures, or would be unlawful (for example if it would constitute 'tipping off' under anti-money laundering legislation) this requirement does not apply.

17.38 The ASPSP must restore access to the AISP or PISP as soon as the reasons for denying access no longer exist.

17.39 Under Regulation 71(8), whenever an ASPSP denies an AISP or a PISP access to a payment account (or payment accounts) it must notify the FCA immediately. We would expect the ASPSP to complete and submit the notification as quickly as possible. Details of the notification requirements can be found in SUP 15.14.8. The notification requirement is also summarised in **chapter 13 – Reporting and notifications**.

Requirements on PISPs, AISPs and CBPIIs

17.40 Many of the requirements on AISPs and PISPs are similar. We set out below the requirements that are common to both AISPs and PISPs, followed by any requirements that are specific to each of those providers. We set out requirements on CBPIIs where relevant (further guidance is provided in **Chapter 8 – Conduct of business requirements**).

Use of security credentials (regulations 69(3)(b) and 70(3)(b))

17.41 AISPs and PISPs are required to ensure that the customer's personalised security credentials are not accessible to other parties (other than the issuer of the personalised security credentials, which is likely to be the ASPSP) and that they are transmitted through safe and efficient channels. We are aware that customers' personalised security credentials can apply to both payment accounts and non-payment accounts. Where a PISP or AISP uses these credentials to access accounts which are non-payment accounts (and are, therefore, not governed by the PSRs 2017 in respect of regulations 69 and 70), we would expect a PISP or AISP to apply the same standards of protection to the personalised security credentials (e.g. transmitting them through safe and efficient channels) as they would when transmitting them in respect of payment accounts. Without this, the personalised security credentials which are used to access payment accounts would not benefit from the protections under the PSRs 2017 and the SCA-RTS. Businesses must also comply with other legal or regulatory requirements relating to data protection.

Explicit consent (regulations 68(3)(a), 69(2), 69(3)(c) and 70(3)(a))

17.42 AISPs must not provide AIS without the customer's 'explicit consent' to do so. Similarly, payment initiation services require the payer's explicit consent to execute a payment transaction. PISPs must not pass information to any person except a payee and then only with the payer's 'explicit consent'. Further, ASPSPs must have the

customer's 'explicit consent' before responding to CBPII requests for confirmation of availability.

17.43 ASPSPs, AISPs and PISPs should have regard to the Information Commissioner's Office guidance on 'explicit consent' keeping the objectives and specific context of the PSRs 2017 in mind. We expect PISPs/AISPs to be able to evidence their customers' explicit consent.

In order to enable customers to give 'explicit consent', AISPs and PISPs should make available to customers the information needed to make an informed decision and understand what they are consenting to (e.g. they must be able to understand the nature of the service being provided to them and the way that their information will be used). In the case of PIS, explicit consent is given by the customer when they initiate a payment by using a PISP. The initiation of the payment by the PISP and the transmission of the customer's encrypted credentials through the required safe and efficient communication channels demonstrates explicit consent to the ASPSP.

17.44 It is the AISP/PISP's responsibility to ensure that the customer has received sufficient information in order to give consent. ASPSPs are not required to check the terms of the consent provided by the customer, except in the case of CBPIIs.

Identification and communication with the ASPSP (regulation 68(3) (c), 69(3)(d) and 70(3)(c))

17.45 Regulation 68(3)(c), 69(3)(d) and 70(3)(c) apply 18 months after the SCA-RTS is published in the Official Journal of the European Union. Once this happens both AISPs and PISPs must identify themselves to the ASPSP each time they initiate a payment order or for each communication session. CBPIIs must authenticate themselves towards the ASPSP before each confirmation request. We expect the SCA-RTS to contain the detail regarding how such identification or confirmation must take place.

17.46 CBPIIs, PISPs and AISPs are also obliged to communicate in accordance with the SCA-RTS. We expect the SCA-RTS to contain a number of requirements in relation to the method of communication used by the CBPII, PISP and AISP. In relation to whichever method of access AISPs/PISPs use, they must be able to meet all of the requirements in the PSRs 2017 and the SCA-RTS (e.g. AISPs must access information only from designated payment accounts).

Sensitive payment data (regulations 69(3)(e) and 70(3)(e))

17.47 PISPs are not permitted to store sensitive payment data of the customer. AISPs are not permitted to request or store sensitive payment data linked to the payment accounts they access.

17.48 Sensitive payment data are defined as "information, including personalised security credentials, which could be used to carry out fraud". In relation to AIS and PIS, they do not include the name of an account holder or an account number.

17.49 In our view, for PISPs this primarily means that they must not store a customer's personalised security credentials. An AISP can store personalised security credentials if it is necessary in order to provide the account information service, as they were obtained from the customer rather than the payment account accessed.

17.50 Where a payment service provider is providing AIS and PIS, the provider is not permitted to use sensitive payment data obtained for the purposes of the account information service when it is providing the payment initiation service.

Requesting information (regulations 69(3)(f) and 70(3)(f))

17.51 AISPs and PISPs are not permitted to request any information from the payer except information required to provide the payment initiation or account information service.

17.52 As a general principle, we take this to mean that PISPs and AISPs should not request more information than is absolutely necessary to provide the specific service that they offer to their customers. For AISPs, in particular, this will depend on the nature of the service. For example, if an AISP provided detailed analytics of a customer's spending habits, that AISP would need to request more information than an AISP providing a service which frequently updated the customer on their balances on various accounts. We would not expect many PISPs acting on behalf of merchants for single payment transactions to need information on a customer's transactions or balance.

Using, accessing and storing information (regulations 68(8)(a), 69(3)(g) and 70(3)(g))

17.53 PISPs and AISPs are not permitted to use, access or store any information for any purpose except for the provision of the account information or payment initiation service explicitly requested by the customer.

17.54 PISPs are able to provide information to payees, but it is not the role of PISPs to access account information. Where PISPs pass information to payees about payers, we take this to mean information which would usually be given as part of a similar transaction (e.g. delivery address, confirmation that the payment has been made) made directly by the payer.

17.55 Generally speaking, it is our view that AIS and PIS should be offered in a way which ensures that customers benefit from high standards of data security and in full conformity with any relevant rules, including applicable data protection law, SYSC and other systems and control requirements.

17.56 CBPIIs are not permitted to store any confirmation received from the ASPSP or use it for any purpose other than for the execution of the card-based payment transaction.

Other requirements applicable to PISPs

Holding funds of a payer (regulation 69(3)(a))

17.57 A PISP must not hold the payer's funds in connection with the provision of the payment initiation service at any time.

Not changing the payment order (regulation 69(3)(h))

17.58 A PISP must not 'change the amount, the payee or any other feature of the transaction'. We take this to mean that PISPs must not change any details of a transaction as presented and explicitly consented to by the customer. This does not, however, prevent PISPs from pre-populating the payment order for the customer.

Other requirements applicable to AISPs

Access to information (regulation 70(3)(d))

17.59 AISPs must not access any information other than information from designated payment accounts and associated payment transactions. We expect the SCA-RTS to require AISPs to have in place mechanisms to ensure that they do not access information from payment accounts which the customer has not designated. This is intended to give customers control over what is being accessed by an AISP.

Requirements on ASPSPs, CBPIIs, PISPs and AISPs when communicating and interacting with their customers in relation to these services

17.60 In **Chapter 8 – Conduct of Business** we have included guidance on our expectations on ASPSPs, CBPIIs, AISPs and PISPs in relation to the provision of information to customers. In summary, in addition to compliance with the guidance above, we expect:

- CBPIIs, AISPs and PISPs to provide or make available clear information to customers about the way that their service works and how information will be used – see paragraph 8.115 of **Chapter 8 – Conduct of business requirements**;
- PISPs and ASPSPs to make available to customers clear information about the notification process where the customer becomes aware of an unauthorised or incorrectly executed transaction – see paragraph 8.117 of **Chapter 8 – Conduct of business requirements**.

17.61 ASPSPs, CBPIIs, AISPs and PISPs also need to be aware of their obligations under data protection law and under consumer protection law, such as the Consumer Protection from Unfair Trading Regulations 2008 which prohibit unfair, misleading and aggressive practices.

Transitional arrangements before the RTS enter into force

17.62 In relation to certain provisions, there is a transitional period beginning on 13 January 2018 and ending 18 months after the date the SCA-RTS enters into force. During that transitional period, ASPSPs, CBPIIs, PISPs and AISPs are required to comply with regulations 68, 69 and 70 of the PSRs 2017, except for regulations 68(3)(c), 69(2)(a) and (3)(d), 70(2)(a) and (3)(c) and 100 which depend on the SCA-RTS and apply at the same time as the SCA-RTS.

17.63 This means that AISPs and PISPs are, for example, still required to transmit personalised security credentials through safe and efficient channels. In this regard, we expect CBPIIs, AISPs and PISPs to ensure, for example, that they have taken all reasonable measures to guard against the risk of the personalised security credentials being extracted from their systems or caught in transit in a usable form and that systems are in place so that personalised security credentials cannot be accessed by employees.

17.64 From 13 January 2018, ASPSPs can deny an AIS or PIS access to a payment account only if the conditions in regulation 71(7) of the PSRs 2017 are met (see 17.33 – 17.39). Firms will have to notify us of their denial of access and the grounds for denial. We will assess these reports and take such measures as we consider to be appropriate.

17.65 In advance of the date on which the SCA-RTS becomes applicable, where an ASPSP provides a PSRs 2017 compliant means for AISPs and PISPs to provide those services in relation to payment accounts accessible online, the ASPSP is not required to provide another alternative means of access to those payment accounts. However, the ASPSP must not block or obstruct the use of AIS and PIS for the accounts they are servicing. ASPSPs are free to provide multiple interfaces for access, provided at least one of these complies with the PSRs 2017 (including the SCA-RTS when it becomes applicable).

17.66 During the period before the SCA-RTS becomes applicable, the parties may find it helpful to take account of industry standards[36] which are being developed as a result of the Competition and Markets Authority's Open Banking Remedy[37].

[36] More information on Open Banking delivery can be found here https://www.openbanking.org.uk/2017/03/13/platform-distributing-bank-product-branch-atm-data-available/

[37] The final report of the Competition and Markets Authority's (CMA) retail banking market investigation was published on 9 August 2016 https://www.gov.uk/government/news/cma-paves-the-way-for-open-banking-revolution

18. Operational and security risks

Under Article 95 of PSD2, the European Banking Authority is tasked with the development of Guidelines on operational and security risks under PSD2.

When the Guidelines are approved by the EBA's Board of Supervisors, the EBA will publish them, and any other required documentation, on its website. The Guidelines are formally issued once they are published in all the official EU languages on the EBA website.

We will update this chapter once the Guidelines have been published in the Official Journal.

19. Financial crime

This chapter and any other reference to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, the Money Laundering Regulations or the 'MLRs' in this draft guidance is subject to amendment, pending the outcome of consultation on the Money Laundering Regulations by HM Treasury.

Introduction

19.1 All PSPs and e-money issuers must comply with legal requirements to deter and detect financial crime, which includes money laundering and terrorist financing.

19.2 Relevant legislation includes:

- the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017(MLRs)
- the EU Funds Transfer Regulation[38]
- section 21A of the Terrorism Act 2000
- the Proceeds of Crime Act 2002
- the relevant financial crime provisions of the PSRs and EMRs (including those relating to the management of security risks and the application of strong customer authentication)
- Schedule 7 to the Counter-Terrorism Act 2008

19.3 PSPs and e-money issuers are also subject to the various pieces of legislation that implement the UK's financial sanctions regime[39]

19.4 Credit institutions that provide payment services and issue e-money are subject to legal requirements and relevant provisions in our Handbook, including the provisions relating to financial crime in our Senior Management Arrangements, Systems and Controls (SYSC) sourcebook in SYSC 6.1.1 R and SYSC 6.3.

19.5 Authorised PIs, authorised EMIs and RAISPs who wish to provide payment services (or distribute or redeem e-money in the case of authorised EMIs) through an establishment in another EEA state in accordance with **Chapter 6 – Passporting**, must comply with the relevant anti-money laundering and counter terrorist financing laws enacted in that Member State. Firms should check what their obligations will be in the host state and take steps to comply with that law.

---

[38] EU Regulation 847/2015 makes changes to the rules on wire transfers previously set out in EU Regulation 1781/2006.

[39] More detail on the UK's financial sanctions regime is available from the Office for Financial Sanctions Implementation (OFSI) https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation.

19.6 In certain circumstances host Member States may require, under Regulatory Technical Standards developed by the European Banking Authority under the fourth Money Laundering Directive, the appointment of a central contact point in the host member state for anti-money laundering and counter terrorist financing purposes.[40] PSD2 also contains separate provisions relating to the power of host Member States to require the appointment of a central contact point for supervisory purposes where a PI is exercising establishment passport rights using agents. This is discussed in **Chapter 6 - Passporting**.

Application to become a PI or EMI

19.7 **Chapter 3 – Authorisation and registration** outlines the authorisation and registration requirements relating to financial crime for PIs and EMIs.

Systems and controls

19.8 We expect all PSPs and e-money issuers to establish and maintain systems and controls to comply with their legal obligations relating to financial crime under the PSRs 2017, the EMRs and (where we are the supervisory authority) under the legislation referred to above. These systems and controls include appropriate and risk-sensitive policies and procedures to deter and detect financial crime and an organisational structure where responsibility to prevent financial crime is clearly allocated.

19.9 The FCA has produced guidance on preventing financial crime – Financial Crime: a guide for firms that will be relevant for PSPs and e-money issuers. For PIs who are subject to supervision by HMRC under the MLRs, HMRC has also provided guidance - Anti-money laundering guidance for money service businesses. **Chapter 12 – Supervision** provides a more detailed outline of our supervisory role and that of HMRC in relation to PIs registered with it under the MLRs).

Policies and procedures

19.10 EMIs, PIs and RAISPs (under the MLRs) are required to demonstrate that they establish and maintain appropriate and risk-sensitive policies and procedures for countering the risk that they may be used to further financial crime. Appropriate policies and procedures are proportionate to the nature, scale and complexity of the EMI's, PI's, or RAISPs activities and enable it to identify, assess, monitor and effectively manage financial crime risk to which it is exposed.

19.11 In identifying its financial crime risk, an EMI, PI or RAISP should consider a range of factors, including (where they are relevant):

- its customers, product and activity profile;
- its distribution channels;
- the type, complexity and volume of permitted transactions;

[40] EBA Consultation Paper on Joint draft Regulatory Technical Standards on the criteria for determining the circumstances in which the appointment of a central contact point pursuant to Article 45(9) of Directive (EU) 2015/849 is appropriate and the functions of the central contact point, published 10 February 2017, available here: http://www.eba.europa.eu/-/esas-consult-on-the-establishment-of-central-contact-points-to-strengthen-fight-against-financial-crime

- its processes and systems; and
- its operating environment.

19.12 As part of their risk assessment and to mitigate the risk of their products being used for purposes connected with financial crime, we expect EMIs, PIs and RAISPs to:

- where applicable, apply ongoing due diligence to customers on a risk-sensitive basis in accordance with their obligations under the MLRs; and
- put in place and enforce policies to determine the acceptable use of their products.

19.13 EMIs and PIs that provide payment or e-money services to merchants should consider whether any special risk mitigation measures are necessary for these customers. This is because merchants can be involved in activities that are associated with an increased risk of money laundering. EMIs and PIs should also be alert to the possibility that merchants may abuse their products to further illegal activity, such as the sale of child abuse images or age-restricted goods to minors.

19.14 EMIs, PIs and RAISPs (where appropriate) should carry out regular assessments of their financial crime policies and procedures to ensure they remain relevant and appropriate. As part of this, EMIs, PIs and RAISPs should be alert to any change in their operating environment that will have an impact on the way they conduct their business. For example, we expect EMIs, PIs and RAISPs to be alert to the publication of any information on financial crime risks and threats associated with e-money products or payment services, such as typology reports from the Financial Action Task Force or other relevant domestic and international bodies, and incorporate this information in their risk assessment as appropriate.

19.15 Under regulation 36 of the EMRs and regulation 36 of the PSRs 2017, EMIs and PIs are ultimately responsible for anything done or omitted by any of their employees, agent (and distributors in the case of EMIs), branch or outsourced provider to the same extent as if they have expressly permitted it. This includes a failure to take adequate measures to prevent financial crime. EMIs and PIs must be aware of this risk and take measures to manage it effectively. This includes taking steps to satisfy themselves of employees', agents', distributors' and third parties' ongoing compliance with their financial crime obligations.

19.16 **Chapter 5 – Appointment of agents** contains further detail on the responsibility of EMIs and PIs for their agents and distributors.

19.17 EMIs and PIs should also take steps to ensure that they comply with the UK's financial sanctions regime.

Internal organisation

19.18 We expect EMIs, PIs to establish a clear organisational structure where responsibility for the establishment and maintenance of effective policies and procedures to prevent financial crime is clearly allocated.

19.19 Regulation 21(1) of the MLRs requires EMIs, PIs and RAISPs (where appropriate) to appoint an individual who is a member of the board of directors (or equivalent) as the officer responsible for compliance with the MLRs. Regulation 21(7) specifically requires electronic money issuers to appoint an individual to monitor and manage compliance with, and the internal communication of, the policies, procedures and controls relating to the matters referred to in regulation 19(3)(a) to (e) of the MLRs. The person appointed under either of these regulations may be the same person who is also the officer nominated under the Proceeds of Crime Act 2002. We expect the individual appointed to have the knowledge, experience and training as well as a level of authority and independence within the EMI or PI and sufficient access to resources and information to enable him/her to carry out that responsibility.

Industry guidance

When considering whether a breach of applicable legislation in relation to anti-money laundering and counter-terrorist financing has occurred, we will consider whether an EMI or PI has followed relevant provisions in the guidance for the UK financial sector issued by the Joint Money Laundering Steering Group (JMLSG). EMIs and PIs are reminded that the JMLSG does not intend its guidance to be applied without thought, as a checklist of steps to take.

Enforcement

19.20 Under the EMRs, PSRs 2017 and MLRs, we have powers to take appropriate enforcement action, which may include cancelling, suspending or varying an authorisation or registration, where an institution that fails to meet its obligation to put in place effective procedures in relation to financial crime.

19.21 We may censure or impose a penalty on EMIs, PIs and RAISPs that contravene requirements imposed by or under the EMRs and the PSRs 2017 (as applicable). We may also enforce financial crime obligations under other legislation, including FSMA, the MLRs and Schedule 7 to the Counter-Terrorism Act 2008.

19.22 See **Chapter 14 - Enforcement** for more details about our enforcement approach.

Annex 1- Useful links

Web links are provided below to useful information resources.

Legislation
The Electronic Money Regulations 2011
Payment Services Directive 2
Payment Services Regulations 2017

FCA Handbook
Our Handbook is an extensive document that sets out the FSA's rules and guidance for financial services. There are a few areas of the Handbook that contain rules applicable to payment services. These are as follows:

Glossary
Provides definitions of terms used elsewhere in the Handbook. Clicking on an italicised term in the Handbook will open up the Glossary definition.

General Provisions (GEN) – GEN 2
Contains provisions on interpreting the Handbooks.

Fees manual (FEES)
Contains fees provisions relevant to payment service providers.

Banking: Conduct of Business sourcebook (BCOBS)
From 1 November 2009, banks and building societies are also be required to comply with the conduct of business rules for retail banking in this module of our Handbook.

Supervision manual (SUP) – SUP 9
Describes how people can seek individual guidance on regulatory requirements and the reliance they can place on guidance received.

Decision Procedure and Penalties Manual (DEPP)
Contains the procedures we must follow for taking decisions in relation to enforcement action and setting penalties.

Dispute Resolution: Complaints sourcebook (DISP)

Contains the obligations on PSPs and e-money issuers for their own complaint handling procedures. It also sets out the rules concerning customers' rights to complain to the FOS.

The Handbook website also contains the following regulatory guides that are relevant to payment service providers:

Enforcement Guide (EG)
Describes our approach to exercising the main enforcement powers given to us under FSMA and the PSRs

Financial Crime: a guide for firms
This contains guidance on steps firms can take to reduce their financial crime risk

Perimeter Guidance manual (PERG) – PERG 15
Contains guidance aimed at helping businesses consider whether they need to be separately authorised or registered for the purposes of providing payment services in the UK

Unfair Contract Terms Regulatory Guide (UNFCOG)
Explains our powers under the Unfair Terms in Consumer Contracts Regulations 1999 and our approach to exercising them

Guidance and information

There is also guidance and information issued by us and the Financial Ombudsman Service likely to be relevant to readers of this document.

- Information about how to complain to us about an FCA regulated firm.
- Information about hot to complain about the FCA, PRA or the Bank of England.
- Information about the Financial Ombudsman Service's processes for handling complaints.
- Information from the Financial Ombudsman Service specifically for smaller businesses.

Complaint handling

Dispute Resolution: Complaints sourcebook (DISP)

FCA reporting system for firms

GABRIEL is our regulatory reporting system for the collection, validation and storage of regulatory data.
Connect is our online system that you can use to submit applications and notifications.

Money Laundering Regulations 2007 (MLR)
Information from HMRC about compliance with the MLR.

Annex 2 - Useful contact details

Financial Conduct Authority (FCA)
25 The North Colonnade
Canary Wharf
London, E14 5HS

Contact Centre
0845 606 9966

Consumer Helpline
0845 606 1234

Payment Systems Regulator (PSR)
25 The North Colonnade
Canary Wharf
London, E14 5HS

Contact Centre
0845 606 9966

Consumer Helpline
0845 606 1234

Financial Ombudsman Service
South Quay Plaza
183 Marsh Wall
London, E14 9SR

0845 080 1800 or 020 7964 0500

Her Majesty's Revenue and Customs (HMRC)
National Advice Service
Written Enquiries Section
Alexander House
Victoria Avenue
Southend
Essex, SS99 1BD

0845 010 9000

Annex 3 - Status disclosure sample statements

The following are suggested statements for payment service providers to include in their contracts and correspondence with customers. It is not mandatory to use these exact statements, but it is important that customers are made aware of the payment service provider's authorisation status.

Note that regulation 48 requires — with respect to framework contracts — that customers are provided with the information specified in Schedule 4. This includes details of the payment service provider's regulators, including any reference or registration number of the payment service provider.

There is also a requirement with respect to individual payment service contracts in regulation 43 (2) (e) that the payment service provider gives the information specified in Schedule 4 "as is relevant to the single payment service contract in question". We consider that details of the regulator will be relevant information and expect firms to mention their regulated status.

Firms which require authorisation under both FSMA and the PSRs should reference both authorisations.

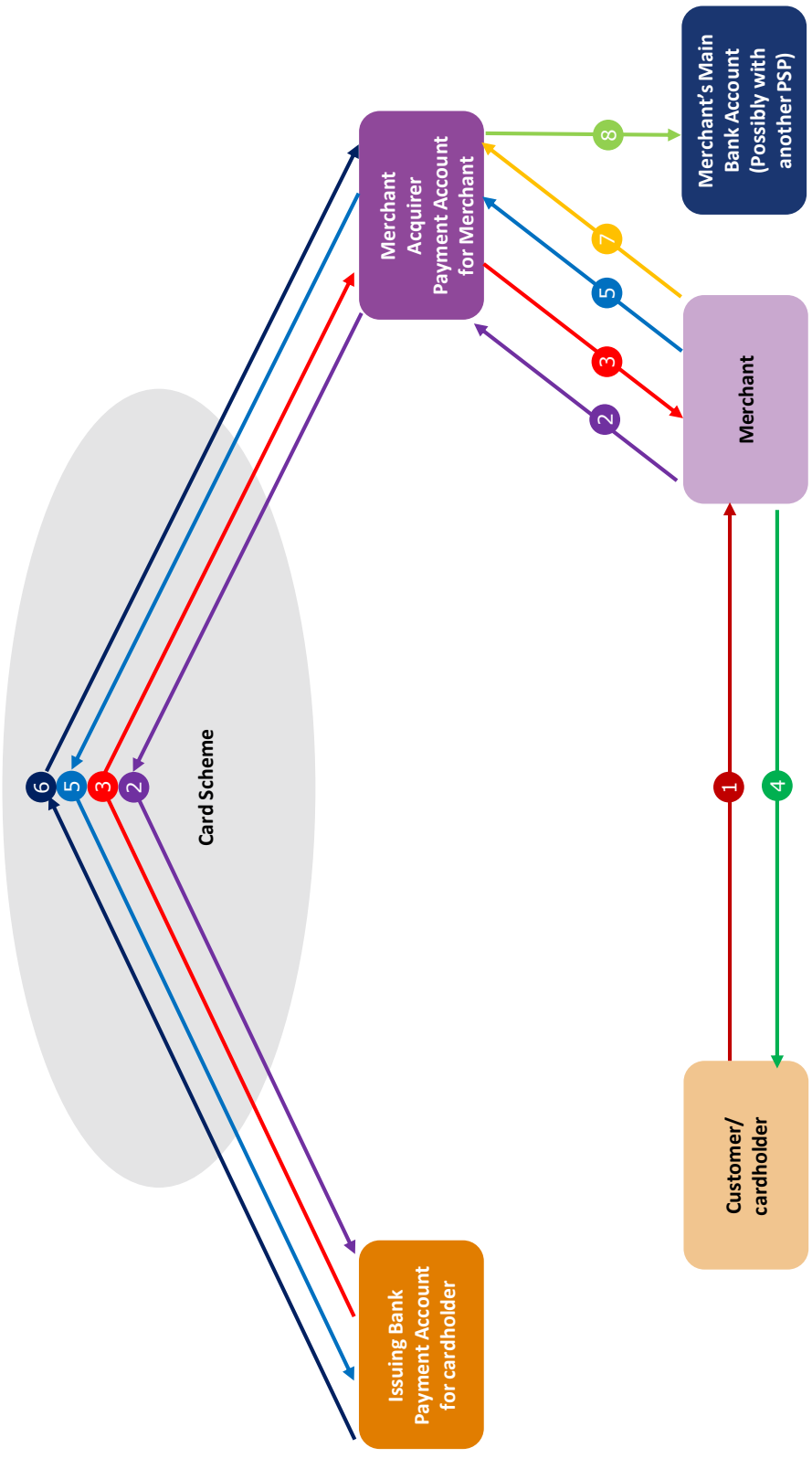
Authorised PIs / Authorised EMIs / RAISPs / Small PIs / Small EMIs

[Name] is authorised by the Financial Conduct Authority under the Payment Service Regulations 2009 [register reference] for the provision of payment services.

EEA Authorised PIs / EEA Authorised EMIs / EEA Authorised RAISPs

Authorised by [name of Home State regulator] and regulated by the Financial Conduct Authority for the conduct of payment services business in the UK.

Annex 4 - merchant acquiring



1) Customer offers card for payment.
2) Merchant seeks authorisation from issuing bank (where required).
3) Issuing bank authorises payment (where required)
4) Merchant provides goods or services to customer
5) Merchant requests Acquirer to transmit payment order(regulation 86: 'within time limits agreed between the payee and his PSP')– Acquirer requests settlement on behalf of Merchant through card scheme
6) Issuing bank makes payment to Merchant Acquirer through card scheme (funds held by Merchant Acquirer (in payment account in name of Merchant))
7) Merchant requests payment from Acquirer to his main account (may be standing instruction–at agreed frequency)
8) Transfer from Merchant Acquirer to Merchant's main account in accordance with contractual agreement

Four-party card scheme

1. The diagram above sets out our understanding of the elements involved in a card transaction with a Merchant accessing the relevant card scheme through a Merchant acquirer. It shows how the Merchant acquirer operating a payment account in the name of the Merchant can hold funds due to a Merchant for a period to allow for chargebacks under the card scheme, before they are remitted to the Merchant's main operational bank account.

2. Under this model, the card issuer authorising the payment is not the beginning of the transaction. Rather, the first payment transaction begins when the Merchant acquirer, as the payee's (Merchant's) PSP, transmits the payment order to the payer's PSP (the card issuer). Under Article 83(3) of PSD2 this must be "within time limits agreed between the payee and the payment service provider". This allows them to agree how frequently such claims are made.

3. The point when the payer's PSP receives this payment order for the purposes of the execution time provisions in the PSRs will be the point at which the card issuer receives the claim. That card issuer is then responsible under regulation 86(1) for ensuring that the funds reach the Merchant acquirer's account by the end of the following business day (D+1).

4. Regulations 86(5) and 89(1) then require the Merchant acquirer, as the payee's (Merchant's) PSP, to value date and make available the funds to the payee's payment account immediately. Under the model set out above, this will be the payment account it operates in its books for the Merchant. This is shown in points 5 and 6 in the diagram above. Our understanding is that Merchant acquirers already effectively run such accounts for the Merchants for whom they operate, although they are not currently labelled as payment accounts, in that they will have details of all the Merchant's transactions, and transfers to the Merchant's main operational bank account on its books.

5. In general terms there is nothing in the PSD2 which prevents firms from operating accounts which have some restrictions, such as minimum balances, or notice periods. In addition, given that there will be a standing instruction to transfer the funds to the Merchant's main bank account, this may be taken as a future dated instruction to transfer the funds "*on a specific day, on the last day of a certain period, or on the day on which the payer has put funds at the disposal of its payment service provider"* (regulation 81(4)). In this way, the funds are already the subject of a payment order, thus fulfilling the requirement that the funds are "at the payee's disposal".

6. So the transfer of the funds from the Merchant's payment account with the Merchant acquirer to the Merchant's main operational bank account will be a separate payment transaction. This is shown in points 7 and 8 above.

7. The funding of the cardholder's payment account is completely separate from the above process, so we have not included it.

8. We are aware that there a number of bureaux or aggregators providing merchant acquiring services in the UK whose position is not reflected in the model described above.

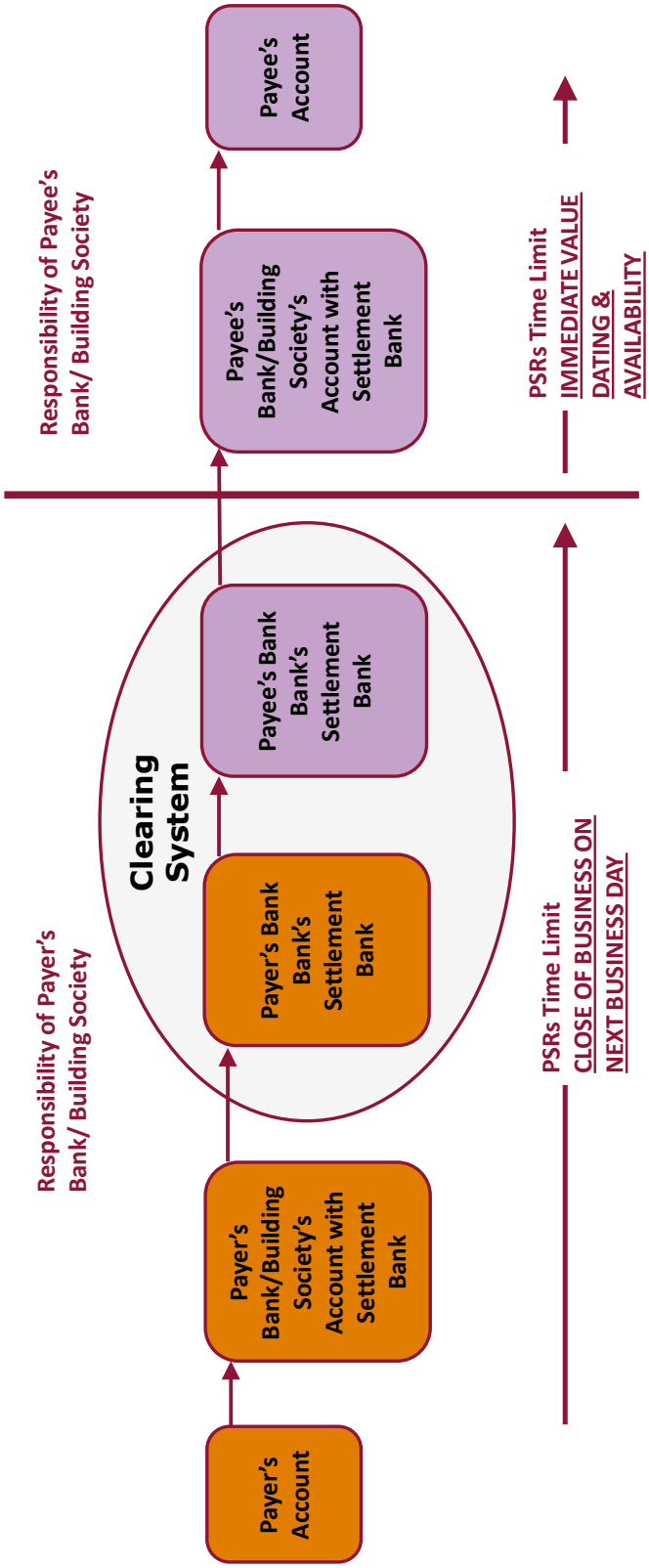
Merchant Acquiring in Three-Party Schemes

9. A three-party card scheme is a card scheme offered by the card issuer, where both the card holder and the merchant are customers of the card issuer. Examples of such schemes are those offered by American Express and Diners Club. These schemes differ from the four-party schemes such as Visa and Master Card in that there is no need for interbank settlement, because both customers (cardholder and Merchant) hold accounts with the card issuer.

10. Transactions under a three-party card scheme are payment transactions under the PSRs, being the act of transferring funds from the payer to the payee.

11. Our understanding is that there are a number of possible organisational structures which a three-party card scheme can take, which may impact upon the particular requirements of the PSRs. Payment service providers operating three-party card schemes are therefore encouraged to contact us at an early stage to discuss their particular circumstances.

Annex 5 - The Payment Process



Glossary of Terms

Many of the terms used in this document are defined in regulation 2 of the PSRs 2017 and are not repeated here. The following information is designed to help make this document more readily understandable.

Financial Services and Markets Act 2000
This is the legislation that gives the FCA its statutory powers.

Small charity
For the purposes of this document, a small charity is one with an annual income of less than £1 million. Such small charities are treated in the same way as consumers under the PSRs. This is the definition used in the PSRs, but note that the term 'charity' is used there instead.

Micro-enterprise
This is an enterprise whose annual turnover and/or balance sheet total does not exceed €2 million (or sterling equivalent) and employs fewer than 10 people.

'Enterprise' means any person engaged in an economic activity, irrespective of legal form and includes, in particular, self-employed persons and family businesses engaged in craft or other activities, and partnerships or associations regularly engaged in an economic activity.

In determining whether an enterprise meets the tests for being a micro-enterprise, account should be taken of the enterprise's 'partner enterprises' or 'linked enterprises' (as those terms are defined in the European Commission's Micro-enterprise Recommendation (2003/361/EC)). An enterprise includes, in particular, a sole trader and family businesses, and partnerships or associations regularly engaged in an economic activity. For example, where one firm holds a majority shareholding in a second firm, if the first firm does not meet the tests for being a micro-enterprise then nor will the second.

One leg transactions
Payment transactions where either the payer or the payee's payment service provider is located outside the EEA.

E-money issuers
In this document, references to e-money issuers are, unless otherwise stated, references to non-bank e-money issuers, including EMIs that are authorised or registered by the FCA.

Upper Tribunal (Financial Services)
The Upper Tribunal (Financial Services) is an independent judicial body established under section 132 of the Financial Services and Markets Act 2000 (FSMA). It hears references arising from decision notices (for example, where the FCA decides to reject authorisation applications) and supervisory notices (for example, where the FCA decides to impose a requirement on a PI's authorisation or registration) issued by the FCA.

Corporate opt-out

Payment service providers may agree with business customers (that is, payment service users who are not consumers, small charities or micro-enterprises) to vary the information they provide from that specified in the PSRs, and, in certain cases, agree different terms in relation to rights and obligations. This is referred to as the 'corporate opt-out'.

Abbreviations and Acronyms

2EMD	Second Electronic Money Directive
Authorised EMI	Authorised electronic money institution
AIS	Account information service
AISP	Account information service provider
Authorised PI	Authorised payment institution
ASPSP	Account servicing payment service provider
ATM	Automated Teller Machine
Bacs	Bacs Payment Schemes Limited
BCOBS	Banking Conduct of Business Sourcebook
Call for Input	February 2016 Call for Input: the FCA's approach to the current payment services regime
CHAPS	Clearing House Automated Payment System
CP	Consultation paper
CONC	Consumer Credit Sourcebook
DEPP	Decision Procedure and Penalties manual
DISP	Dispute Resolution: Complaints
EBA	European Banking Authority
ECN	Electronic Communications Network
EEA	European Economic Area
EG	Enforcement Guide
EMI	Authorised EMIs and small EMIs
EMRs	Electronic Money Regulations 2011
EU	European Union
FSA	Financial Services Authority
FSMA	The Financial Services and Markets Act 2000
FPS	Faster Payments Service
Handbook	The FCA Handbook of Rules and Guidance, available at http://fshandbook.info/
IAP	Indirect Access Provider
Institution	Refers to both PIs and EMIs together
LNE	Limited Network Exclusion
MLRs 2007	Money Laundering Regulations 2007
MLRs 2017	Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
PERG	Perimeter Guidance Manual
PI	Authorised PIs and small PIs
PIS	Payment initiation services
PISP	Payment initiation services provider
PSD	Payment Services Directive

PSD2	The revised Payment Services Directive
PSP	Payment services provider
PSRs 2009	Payment Services Regulations 2009
PSRs 2017	Payment Services Regulations 2017
RAISP	Registered account information service provider
RTS	Regulatory Technical Standard
SCA	Strong Customer Authentication
Small EMI	Small electronic money institution
Small PI	Small payment institution
SUP	Supervision Manual
Treasury	HM Treasury