Payment Services and Electronic Money – Our Approach

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

~~July~~December 2018 (version ~~2~~3)

Approach Document version control

Published on	Changes
19 December 2018 (version 3)	• **New Guidance** on authentication and secure communication under PSD2. Chapters affected 17 and 20. • **Minor changes** to clarify our guidance or reflect legislative change. Chapters affected 1, 3, 6, 8, 13, 18, 19.
5 July 2018 (version 2)	• **New Guidance** on operational and security risks under PSD2. Chapters affected: 13 and 18. • **Minor changes** to clarify our guidance or reflect legislative change. Chapters affected: 3, 4, 5, 10, 15.
19 September 2017 (version 1)	• Changes to the Approach Document to reflect PSD2 and the PSRs 2017.

A tracked marked version is available on our webpage.

How to navigate this document onscreen

returns you to the contents list

takes you to helpful abbreviations

Contents

Preface 3

1 Introduction ~~4~~ 5

2 Scope ~~12~~ 14

3 Authorisation and registration ~~23~~25

4 Changes in circumstances of authorisation or registration ~~58~~ 59

5 Appointment of agents and use of distributors ~~69~~ 70

6 Passporting ~~75~~ 76

7 Status disclosure and use of the FCA logo ~~83~~ 84

8 Conduct of business requirements ~~84~~ 85

9 Capital resources and requirements ~~141~~ 143

10 Safeguarding ~~155~~ 157

11 Complaints handling ~~167~~ 169

12 Supervision ~~175~~ 177

13 Reporting and notifications ~~180~~ 182

14 Enforcement ~~193~~ 196

15 Fees ~~197~~ 200

16 Payment service providers' access to payment account services ~~199~~ 202

17 Payment initiation and account information services and confirmation of availability of funds ~~206~~

209

18 Operational and security risks ~~219~~ 240

19 Financial crime ~~222~~243

20 Authentication 248

Annex 1
Useful links ~~227~~263

Annex 2
Useful contact details ~~229~~265

Annex 3
Status disclosure sample statements ~~231~~266

Annex 4
Merchant acquiring ~~232~~267

Annex 5
The Payment Process ~~235~~ 270

Glossary of Terms ~~236~~ 271

Abbreviations and Acronyms ~~238~~273

Preface

This document will help businesses to navigate the Payment Services Regulations 2017 (PSRs 2017)[1] and 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, which 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. 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~~ In September 2017~~ Approach Document has been updated throughout to reflect the following:~~

~~•~~ , we merged our Approach Documents on the PSRs 2017 and the EMRs to reflect changes brought about by the introduction of the revised Payment ~~Services~~ Services Directive (PSD2),[2]

~~•~~ other changes in the market ~~that have an impact on the~~since our original guidance ~~we first published in 2009 and 2011 respectively~~

~~• the~~ was issued and as a response to feedback received ~~in the course of the~~ to our Call for Input ~~we~~ (published in February 2016

~~• feedback received in the course of CP~~) and to CPs 17/11 ~~(published in April 2017)~~

~~• feedback received in the course of CP~~and 17/22 ~~(published in~~. This Payment Services and Electronic Money Approach Document is referred to hereafter as the "Approach Document".

In July ~~2017)~~

~~Our consultation papers and feedback statements can be accessed~~2018, we published a second version of the Approach Document to incorporate new guidance

on ~~our website. We have merged our Approach Documents on the PSRs 2017 and the EMRs as an outcome of the Call for Input~~operational and security risk under PSD2 and other minor amendments.[3]

1 As amended by the ~~Payment Systems and Services and Electronic Money (Miscellaneous Amendments) Regulations 2017~~Payment Systems and Services and Electronic Money (Miscellaneous Amendments) Regulations 2017, available at www.legislation.gov.uk/uksi/2017/1173/contents/~~made~~made.

2 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36EU and Regulation 1093/2010, and repealing Directive 2007/64/EC.

~~3 Previously, "The FCA's role under the Payment Services Regulations 2009" and "The FCA's role under the Electronic Money Regulations 2011" respectively.~~

3 We consulted on the proposed changes in CP 18/6 (published in March 2018).

This December 2018 version of our Approach Document reflects:

- the finalisation of European regulatory technical standards on passporting and home-host supervision
- the finalisation of European regulatory technical standards on strong customer authentication and common and secure communication and related guidance
- changes to fraud reporting requirements
- minor changes to clarify our guidance

Our consultation papers and feedback statements can be accessed on our website.

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 in the UK. 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.

The payment services and e-money regulatory regime

1.3 PSD2 requires the European Banking Authority (EBA) to produce a number of technical standards and guidelines for the implementation of PSD2. Where relevant, these should be read alongside this document. The EBA will provide further clarifications via use of the EBA's Single Rulebook question and answer tool.[4]

1.4 The Payment Systems Regulator has published a separate Approach Document on the aspects of the PSRs 2017 for which it is solely responsible, 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 (PSD1)[4][5], 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 (EU) Official Journal on 23 December 2015. The full text of ~~the~~ PSD2 can be found on the EU's website. PSD2 replaces PSD1 and updates the regulatory regime to reflect changes in the market and remove barriers to market entry. The main changes are summarised below. PSD2's aims include:

- contributing to a more integrated and efficient European payments market
- levelling the playing field for payment service providers (PSPs)

4 http://www.eba.europa.eu/single-rule-book-qa

5 Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC.

- promoting the development and use of innovative online and mobile payments
- making payments safer and more secure

4 Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC.

- 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 and parts of the Handbook implement PSD2 in the UK. Most PSPs 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 Payment Services Regulations 2009 and make the following changes to the regulatory regime:

- Amend the authorisation and prudential regime for PSPs 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 European Economic Area (EEA) States. Because of their UK authorisation, they have the right to establish or provide services across the EEA.[5] [6] The exercise of passporting rights is amended through the PSRs 2017 as well as the EBA Regulatory Technical Standards on passporting under PSD2.[7] Further information can be found in **Chapters 3 – Authorisation and registration, 6 – Passporting and 9 – Capital resources and requirements**.

- Continue to allow PSPs and e-money issuers operating beneath certain thresholds to be registered instead of obtaining authorisation (regulation 14 of the PSRs 2017 and regulation 13 of the EMRs). Such small PIs and small EMIs are unable to passport. See **Chapter 3 – Authorisation and registration** and **Chapter 6 – Passporting** for further information.

- Continue to exempt certain PSPs (e.g. banks) from PSD2 authorisation and 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 – when they pass a given threshold – are required to notify us. See **Chapter 4 – Changes in circumstances of authorisation and registration** for further information.

6 At the time of publishing this Approach Document, PSD2 has been adopted under scrutiny by the EEA. It has not yet been incorporated into the EEA Agreement or come into force in Norway, Liechtenstein or Iceland. For clarity, we will refer to PSD2 throughout this Approach Document as if it has been incorporated into the EEA Agreement and has come into force in Norway, Liechtenstein and Iceland.

7 Commission Delegated Regulation (EU) 2017/2055 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for the cooperation and exchange of information between competent authorities relating to the exercise of the right of establishment and the freedom to provide services of payment institutions is available here: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R2055&from=EN

- Make changes to the appointment of agents. 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,

5 ~~At the time of publishing this Approach Document, PSD2 has been adopted under scrutiny by the EEA. It has not yet been incorporated into the EEA Agreement or come into force in Norway, Liechtenstein or Iceland. For clarity, we will refer to PSD2 throughout this Approach Document as if it has been incorporated into the EEA Agreement and has come into force in Norway, Liechtenstein and Iceland.~~

banks and building societies need to comply with the ~~Banking: Conduct of Business~~Banking: Conduct of Business Sourcebook (BCOBS). ~~Sourcebook (BCOBS).~~

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

- Make changes to the rules governing the access to payment account services that credit institutions provide to other PSPs. The rules state that access should be proportionate, objective and non-discriminatory (POND). See **Chapter 16 – Payment service providers' access to payment account services** for further information.

- Introduce two new payment services (account information services (AIS) and payment initiation services (PIS)) and set 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.

- Make changes to the rules governing access to payment systems. The rules state that access should be proportionate, objective and non-discriminatory (POND), subject to certain exemptions. See the **Payment Systems Regulator's Approach Document** for further information.

- Introduce new requirements for all PSPs to manage the operational and security risks relating to the payment services they provide. This includes establishing and maintaining effective incident management procedures and submitting reports to us. See **Chapter 18 – Operational and security risks** and **Chapter 13 – Reporting and notifications** for further information.

- Introduce requirements for the security of payments and for communication between PSPs in accordance with the Regulatory Technical Standards on strong customer authentication and common and secure communication (SCA-RTS).[8] See **Chapter 17 – Payment initiation and account information services and confirmation of availability of funds** and **Chapter 20 – Authentication** for further information.

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

8 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN

E-money

1.11 2EMD was published in the EU's Official Journal on 10 October 2009. The full text of 2EMD can be found on the EU's website.[6] 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). It should be noted, however, 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

6 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).

- 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.

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

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

9 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).

1.17 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~~came 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~~are required to provide more information than under the ~~current~~previous 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 the 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

- Professional Indemnity Insurance (PII) or a comparable guarantee held (for businesses that propose providing AIS or PIS)

See **Chapter 3 – Authorisation and registration** and the relevant EBA guidelines and Regulatory 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 additional information. This information must be submitted before 12 April 2018. There are separate provisions that apply to existing authorised PIs and authorised EMIs that wish to provide AIS and/or 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 such activity beyond these dates they ~~will be~~ are required to re-apply to us before 13 April 2018 and 13 October 2018 respectively, and provide any relevant information requested by us. Small PIs and Small EMIs ~~will~~are not ~~be~~ able to provide AIS and/or PIS, and so ~~will~~ need to become

authorised PIs or EMIs if they wish to provide such services. Please refer to **Chapter 3 – Authorisation and registration** for further information.

1.22 Businesses should review the PSRs 2017, particularly regulations 150 to 154 relating to transitional provisions. PSPs ~~will~~ need to comply with the new requirements of PSD2 (introduced through the PSRs 2017 and the Handbook) including conduct of business changes, new complaints handling timeframes and new reporting and notifications from 13 January 2018. Existing PIs and EMIs ~~will~~ need to comply with the majority of the new requirements prior to becoming re-authorised or re-registered. PIs and EMIs should be aware that there are a few exceptions and should review the PSRs 2017 and our Handbook to confirm the start date for each requirement.

1.23 The provisions of the PSRs 2017 which relate to authorisation and registration apply from 13 October 2017. Guidance on these provisions is set out in **Chapter 3 – Authorisation and registration**.

Status of this document

1.24 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.

1.25 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.

1.26 This document supports the legal requirements which are contained in the documents described below. It is essential to refer to the PSRs 2017, the EMRs or relevant parts of the Handbook for a full understanding of the obligations imposed by the regime.

1.27 Guidance is not binding on those to whom the PSRs 2017, EMRs and our rules apply. Rather, guidance is intended to illustrate ways (but not the only ways) in which a person can comply with the relevant regulations and rules. Guidance does not set out the minimum standard of conduct needed to comply with the regulations or our rules, nor is there any presumption that departing from guidance indicates a breach of these. If a firm has complied with the regulations and rules, then it does not matter whether it has complied with guidance we have issued.

1.28 However, 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 SUP 9.4 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.

Rights conferred on third parties (such as clients of a PSP or e-money issuer) cannot be affected by our guidance. Guidance on the PSRs 2017, EMRs or other requirements represents our view, and does common and secure communication to bind the courts, e.g. 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

1.30 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 online:

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

The relevant parts of the FCA Handbook

1.31 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, PIs or RAISPs (unless they are authorised under FSMA in relation to other activities), There are, however, 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 complement the PSRs 2017 and which provisions do not apply to accounts where Parts 6 and 7 of the PSRs 2017 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 PSPs 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 us and the Financial Ombudsman Service relevant to PSPs.

- 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 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.

- Senior Management Arrangements, Systems and Controls sourcebook (SYSC).
  ~~SYSC 9.2~~ SYSC 9.2 includes a record keeping rule relevant to credit institutions providing account information services or payment initiation services.

- 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 PSPs 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 Financial Ombudsman Service.

1.32 The Handbook website also contains the following regulatory guides that are relevant to PSPs:

- 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.

1.33 There is also guidance and information issued by us, the Financial Ombudsman Service and HMRC which is likely to be relevant to readers of this document. This is referenced in the appropriate sections of the document and gathered together in **Annex 1 – Useful links**.

Contacting us

1.34 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.

1.35 **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 Payment Services Regulations 2017 (PSRs 2017). Part II sets out who and what is covered by the Electronic Money Regulations 2011 (EMRs), including what e-money is and information about different types of e-money issuers. Each section sets out where to find further information on scope-related 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 PSPs (see regulations 38, 39, 57, 58 and 61 of the PSRs 2017).

2.3 Chapter 15 of our Perimeter Guidance (PERG)[7]10 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 (PIs)

2.5 The PSRs 2017 establish a class of firms authorised or registered to provide payment services. These are collectively referred to as payment institutions (PIs) in this document. **Chapter 3 – Authorisation and registration** gives details of the procedures for authorisation and registration.

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).

[7]10 https://www.handbook.fca.org.uk/handbook/PERG/15/?view=chapter

Authorised PIs

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

Small PIs

2.9 PSPs which meet the criteria for registration under regulation 14 of the PSRs 2017, and choose to apply for registration rather than authorisation, are referred to as small PIs. Small PIs cannot passport their registration to other EEA States, nor may they provide account information services (AIS) or payment initiation services (PIS). See **Chapter 17 – Payment initiation and account information services and confirmation of availability of funds** and Chapter 15 of PERG for more information about AIS and PIS.

2.10 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**.

Registered Account Information Service Providers

2.11 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 (RAISPs)' and can passport their registration to other EEA States.

2.12 RAISPs are only required to comply with specific parts of the conduct of business requirements. These are identified in paragraphs 8.134 and 8.144 of **Chapter 8 – Conduct of business requirements**.

Agents

2.13 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.

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

Other payment service providers

2.15 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 e-money institutions (Authorised EMIs)
- registered e-money institutions (small EMIs)
- EEA authorised EMIs

- Post Office Limited
- certain public bodies

2.16 These entities must, however, comply with the applicable conduct of business requirements of the PSRs 2017 described in **Chapter 8 – Conduct of business requirements** and the reporting and notification requirements described in **Chapter 13 – Reporting and Notifications**.

2.17 In the case of credit institutions, the relevant application or certification procedures remain those in the Financial Services and Markets Act 2000 (FSMA). Credit institutions are also subject to our rules and guidance in our Banking: Conduct of Business Sourcebook (BCOBS) – see **Chapter 8 – Conduct of business requirements**.

2.18 Credit institutions will need to notify us if they wish to provide AIS or PIS, 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

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

- credit unions
- municipal banks
- The National Savings Bank

2.20 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

2.21 More generally, there is a broad range of activities which do not constitute payment services under Schedule 1 Part 2 of 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 (e.g. bureaux de change);
- payment transactions linked to securities asset servicing (e.g. dividend payments, share sales or unit redemptions);
- certain services provided by technical service providers;
- 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, resulting from services provided by a provider of electronic communication networks or services ("electronic communications exclusion").

2.22 Chapters ~~3A[8]~~3A[11] and 15 of PERG provide more information on these exclusions. **Chapter 13 – Reporting and Notifications** provides information about notifications required from businesses operating under the limited network exclusion and the electronic communications exclusion.

Registers

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

- UK authorised PIs and EMIs, their EEA branches and their agents
- UK registered small PIs and small EMIs and their agents
- UK registered 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

2.24 The European Banking Authority (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 States. This will be available free of charge on the EBA's website.

Payment services

2.25 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 activities likely to be payment services. 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 PERG.

2.26 In addition to questions and answers providing further information on payment ser vices, 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**.

~~8~~11 https://www.handbook.fca.org.uk/handbook/PERG/3A/?view=chapter

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, e.g. 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 PSP or with another PSP • 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 PSP (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
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 supported by the presentation of account information • 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

2.27 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.

2.28 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.

2.29 Where we refer to 'one leg transactions' below, we mean those where either the payer's or the payee's PSP (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 PSPs are (or the sole PSP 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 Financial Ombudsman Service (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 and transactions in non-EEA currencies, 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 and transactions in non-EEA currencies, 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 PSP's account will not apply to one leg in transactions for transactions in non-EEA currencies.

Part II: EMRs

Who the EMRs cover

2.30 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 regulation 3(a) and 3(b) of the EMRs).

2.31 Chapter 3A of PERG gives guidance for firms who are unsure whether their activities fall within the scope of the EMRs.

2.32 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

2.33 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
- not excluded by regulation 3 of the EMRs (see paragraph 2.35 below)

2.34 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

2.35 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 communications exclusion).

How the EMRs define e-money issuers

2.36 The term 'e-money issuer' refers to anyone issuing e-money and should be distinguished from the term 'e-money institution', which refers to the type of regulated entity, rather than the activity. E-money issuers are defined in the EMRs as any of the following persons when they issue e-money.

E-money institutions (EMIs)

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

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

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

2.40 EMIs that meet the criteria for registration under regulation 12 of the 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.

2.41 All EMIs must comply with the conduct of business requirements of the PSRs 2017 and EMRs described in **Chapter 8 – Conduct of business requirements** and the reporting and notification requirements described in **Chapter 13 – Reporting and Notifications**.

EEA authorised EMIs

2.42 Persons authorised in an EEA State other than the UK 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 the second Electronic Money Directive (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

2.43 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 a 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

2.44 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.

2.45 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 Financial Ombudsman Service.

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

Use of Agents and Distributors

2.47 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.

2.48 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 State by engaging distributors, EMIs will need to provide details of distributors in their passporting notification (see **Chapter 6 – Passporting**).

EMIs providing payment services

2.49 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, and EMIs who wish to offer unrelated payment services may have to provide additional information at the point of authorisation (see **Chapter 3 – Authorisation and Registration** for further information). This will primarily be relevant where the EMI wishes to offer payment services that are independent from its e-money products. Where the EMI proposes simply to transfer funds from e-money accounts, such as where a customer uses their e-money to pay a utility bill, this payment service would relate to the activity of issuing e-money.

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

EMIs providing AIS and PIS

2.51 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 Payment Services Regulations 2017 (PSRs 2017) and Electronic Money Regulations 2011 (EMRs) dealing with:

- authorisation of payment institutions (authorised PIs) and e-money institutions (authorised EMIs) (Part I)
- registration of small payment institutions (small PIs) and small e-money institutions (Small EMIs) (Part II)
- registration of businesses only providing account information services (registered account information services providers – RAISPs) (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 registered account information service provider (RAISP), unless it is already another type of payment service provider (PSP) or is exempt or excluded.

3.4 Being a small PI is an option available to businesses with an average payment transactions turnover that does not exceed €3 million per month and which do not provide account information services (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 nor may they provide AIS or PIS. The conduct of business requirements still apply, as does access to the Financial Ombudsman Service by small PIs' eligible customers (see **Chapter 11 – Complaints ~~Handling~~handling** for more information on access to the Ombudsman Service).

3.5 A UK business (or a UK branch of a business with its head office outside the European Economic Area (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 of the Financial Services and Markets Act 2000 (FSMA) to issue e-money or is exempt. Being a small EMI is an option available to UK businesses whose total business activities are projected to generate average outstanding e-money that does not exceed €5 million. There are no passporting rights for small EMIs.

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~~ For EEA-authorised

EMIs with their head office in the EEA this includes payment services that are unrelated to the issuance of e-money, however, small EMIs are not permitted to provide AIS or PIS. If a small EMI

provides payment services unrelated to the issuance of e-money, the limits on payment volumes are the same as for a small PI (i.e. 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 4 – Changes in circumstances of authorisation and registration** for more on how such applications should be made). ~~Small EMIs cannot provide AIS or PIS.~~

3.7 Agents can be appointed by a PI, RAISP or EMI (the principal) to provide payment ser vices on the principal's behalf. The principal accepts responsibility for the acts and omissions 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 applications (see **Chapter 6 – Passporting**).

3.9 The 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~~The Register includes information about PIs, RAISPs and EMIs~~,~~ and their agents and ~~their~~ the EEA branches~~,~~ of PIs and ~~RAISPs.~~
EMIs. This information is also included on a register maintained by the European Banking Authority (EBA), together with information provided by the competent authorities in other EEA States. This is available free of charge on the EBA's website.

Making an application for authorisation or registration

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 (more information is available in **Chapter 15 – Fees**). Applicants that wish to operate through agents will be charged an additional application fee.

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.

~~**3.12** Applicants that wish to operate through agents will be charged an additional application fee.~~

Information to be provided and EBA ~~guidelines~~Guidelines

3.~~13~~12 The EBA has issued 'Guidelines on the information to be provided for authorisation of payment institutions and e-money institutions and registration as account information service providers' (EBA Guidelines).[9]~~12~~ The EBA Guidelines specify the information that applicants for authorisation as a PI or an EMI or registration as a RAISP will be required

9 Available at https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-authorisation-and-registration-under-psd2

to submit. Details on these requirements are set out below in Part I for authorised PIs and authorised EMIs and in Part III for RAISPs. In some cases we will also apply-

12 Available at: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-authorisation-and-registration-under-psd2

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~~13 Where we do not prescribe the format of information that must be given to us, we will need to have enough information to be satisfied that the applicant meets the relevant conditions. This does not mean that the applicant needs to enclose full copies of all the procedures and manuals with their application; 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 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~~14 As set out in the EBA Guidelines, the information provided by the applicant should be true, complete, accurate and up to date. The level of detail should be proportionate to the applicant's size and internal organisation, and to the nature, scope, complexity and riskiness of the particular service(s) the applicant intends to provide.

~~3.16~~ ~~We will acknowledge that we have received an application, and the case officer assigned to deal with it will be in contact soon after.~~ We would expect applicants to answer questions in full in the application form, which includes providing the requested information in bullets under each question.

3.15 We will assess the information provided 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 in writing for more information. We will confirm 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.~~17~~16 Applicants should note that under regulation 142 of the PSRs 2017 and regulation 66 of the EMRs it is a criminal offence to knowingly or recklessly give information that is materially false or misleading in their application.

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

3.~~18~~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, applicants will need to provide information promptly to avoid delay to consideration of their application (see 'Timing'~~ applications are incomplete (when they do not have all the information we need), we will ask in writing for more information. We will then confirm the date from which we consider the application to be complete. The timings set out in Part IV of this chapter~~)~~ will run from that date.

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

3.~~19~~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.

3.20<u>19</u> The <u>applicant should</u> notif~~ication must include~~<u>y the case officer assigned to the application of</u> details of

the change<u>, and provide</u> 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.

~~**3.21** 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.~~22~~20 This section applies to businesses that wish to become an authorised PI or an authorised EMI.

3.~~23~~21 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 EMI are set out in regulation 6 of the EMRs have been met.

3.~~24~~22 The information requirements for applications can be found in Schedule 2 of the PSRs 2017 and section 4.1 of the EBA Guidelines (the API Guidelines) for authorised PIs and Schedule 1 of the EMRs and section 4.3 of the EBA Guidelines (the EMI Guidelines) for authorised EMIs.

3.~~25~~23 There is an application fee for firms looking to become an authorised PI or an authorised EMI (more information is available in **Chapter 15 – Fees**).

3.~~26~~24 For authorised PIs and authorised 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. These are 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.~~27~~25 Authorisation will not be granted unless we are satisfied that the conditions specified in regulation 6 of the PSRs 2017 or regulation 6 of the EMRs (as applicable) have been met.

3.~~28~~26 This section needs to be read alongside the API Guidelines or the EMI Guidelines, as appropriate. Together, the PSRs 2017, API Guidelines, EMRs and 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.~~29~~27 For authorised PIs, API Guideline 3 sets out the information and documentation which needs to be provided for the programme of operations. For authorised EMIs, this is set out in EMI Guideline 3.

3.~~30~~28 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 of 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). Applicants for authorisation as an EMI must also provide an indication of the e-money services the applicant intends to provide (issuance, redemption, distribution). Guidance on e-money activities can be found in Chapter 3A of PERG. The applicant should also describe any other business activities it provides.

3.~~31~~29 The applicant is also required to state whether they will enter into the possession of customers' funds. In our view, being in possession of funds includes an entitlement to funds in a bank account in the applicant's name, funds in an account in the applicant's name at another PI or EMI and funds held on trust for the applicant.

3.~~32~~30 The applicant is required to provide details of how transactions will be executed (including details of all the parties involved in the provision of the services). We may ask for further information, which may include a request to see copies of draft contracts between the applicant and other parties involved in the provision of the services, as well as copies of draft framework contracts. See **Chapter 8 – Conduct of business requirements** for more information on framework contracts and other conduct requirements.

3.~~33~~31 Where the applicant intends to provide AIS or PIS, we would expect the information on the programme of operations to cover the nature of the service being provided to the customer, how their data will be used, and how the applicant will obtain appropriate consent(s) from the customer. See **Chapter 17 – Payment initiation and account information services and confirmation of availability of funds** for more information.

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

3.~~34~~32 API Guideline 4 and EMI Guideline 4 set out the information and documentation which needs to be provided in the business plan.

3.~~35~~33 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.~~36~~34 In accordance with regulation 7(4) of the PSRs 2017 and regulation 7(4) of the EMRs, where an applicant wishes to carry on 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 super vise 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.~~37~~35 As per EBA Guideline 4.2, the business plan should contain information on, and calculation of, own funds requirements. Guidance can be found on own funds in

Chapter 9 – Capital resources and requirements. Applicants should refer to the EBA Guidelines for other business plan requirements, including income information, marketing plan and budget forecasts.

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

3.~~38~~ 37 Where the applicant intends to provide AIS, the information provided should include how the use of customer data fits into the applicant's business model.

Structural organisation (paragraph 12 Schedule 2 of the PSRs 2017, paragraph 7 Schedule 1 EMRs) and close links (regulation 6(9) and (10) of the PSRs 2017 and regulation 6(8) and (9) of the EMRs)

3.~~39~~ 38 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 including through any branches, agents and distributors. API Guideline 5 and EMI Guideline 5 set out the information and documentation which must be provided in relation to the structural organisation.

3.~~40~~ 39 The information must include a description of the applicant's relevant outsourcing arrangements (if any). We may ask for further information, which may include a request to see draft contracts with parties to whom operational functions are outsourced (see section 18.9 on outsourcing). 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 EMI's 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, are 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 require removal or variation

~~**3.41** We will take these factors into consideration when assessing an authorisation application where the business intends to outsource important operational functions.~~

~~**3.42**~~ **40** Regulation 25(3) of the PSRs 2017 and regulation of the 26 of the 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 e-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. We will take these factors into consideration

when assessing an authorisation application where the business intends to outsource important operational functions.

3.~~43~~ 41 Applicants must also 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 (in accordance with regulation 6(9) and (10) of the PSRs 2017 and regulation 6(8) and (9) of the EMRs).

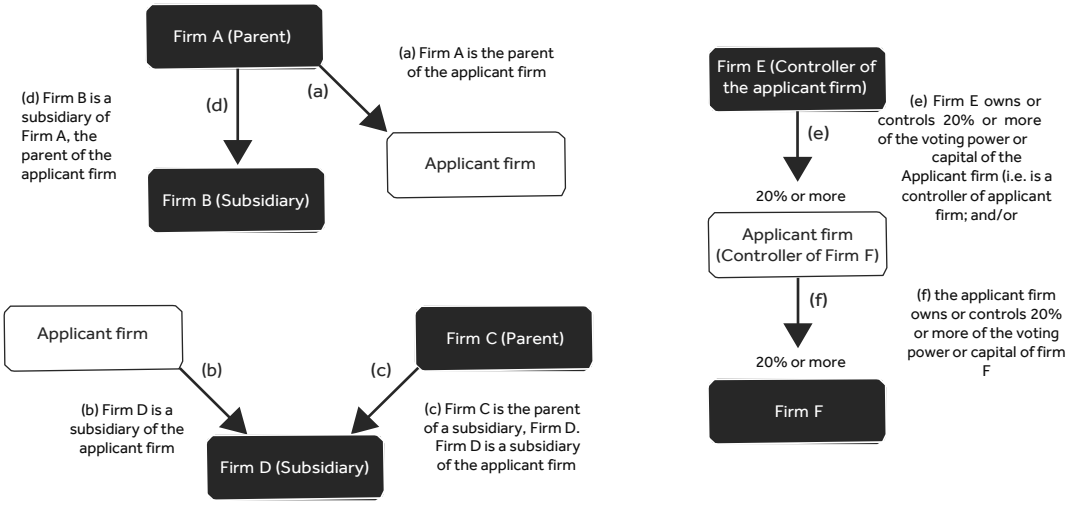
3.~~44~~ 42 A close link is defined as:

- 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.~~45~~43 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.~~46~~44 The following diagram sets out the types of relationships between firms and individuals that meet the definition of a close link. Red shaded boxes are all close links of the relevant applicant firm.



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

3.~~47~~45 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 of the PSRs 2017 or Part 1 of Schedule 2 of the EMRs as the case may be. API Guideline 6 and EMI Guideline 6 set out the information and documentation to be provided as evidence of initial capital.

3.~~48~~46 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.~~49~~ 47 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 3 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 ~~under~~ in Schedule 1 Part 1(1)(a) to (1)(e)	€125,000

3.~~50~~48 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~~ most recent financial statements or 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.

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

3.~~51~~49 An applicant to be an authorised PI must be a body corporate (e.g. a limited company or limited liability partnership) constituted under the law of the UK and whose head of fice (and, where relevant, its registered office) is in the UK.

3.~~52~~50 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, or
- 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.~~53~~51 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, and

- the central administrative functions of the firm (e.g. central compliance, internal audit)

3.~~54~~52 For the purpose of regulation 6(4) of the PSRs 2017, a 'virtual office' in the UK does not satisfy this condition.

3.~~55~~53 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 e-money and payment service business in the UK.

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

3.~~56~~54 Applicants are required to satisfy us that they have taken adequate measures for the purpose of safeguarding users' 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.~~57~~55 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 only.

3.~~58~~56 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.

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

3.~~59~~57 Where an applicant for authorisation as a PI seeks permission to provide PIS or AIS, it must satisfy us that it holds appropriate PII or a comparable guarantee.

3.~~60~~58 Authorised EMIs who intend to provide either PIS or AIS will also need to hold the required PII or a comparable guarantee. 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 of the EMRs that the applicant will not undertake these activities. The applicant can apply to vary its authorisation at a later date (see **Chapter 4 – Changes in circumstances of authorisation or registration**).

3.~~61~~59 API Guideline 18 and EMI Guideline 18 set out the information and documentation that is required for this PII or comparable guarantee. The required PII or comparable guarantee must meet or exceed the minimum monetary amount directed by us from time to time. For this purpose, we direct that the minimum monetary amount
is the amount calculated in accordance with the "Guidelines on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance or other comparable guarantee under article 5(4) of Directive (EU) 2015/2366 (PSD2)" published by the EBA under article 5(4) of PSD2 on 7 July 2016 (EBA-GL-2017-08).

3.60 Applicants should provide the PII calculations and a copy of the terms of the policy proposed, which must comply with the requirements of the PSRs 2017 and EMRs. We would expect the policy to be specifically tailored to address the liabilities set out in

regulation 6(7)(e) and (f) of the PSRs 2017 as regards provision of AIS and PIS. It should cover liability to third parties arising not only from external attacks, but also from any act or omission, including where dishonest, fraudulent or malicious, committed by employees, including directors, officers and partners (in their capacity as employees), and sub-contractors or outsourcers for whose conduct the applicant is legally responsible.

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

3.~~62~~61 Applicants must satisfy us that their governance arrangements, internal control mechanisms and risk management procedures meet the conditions set out in regulation 6(6) of the PSRs 2017 or regulation 6(5) of the EMRs. API Guideline 8 and EMI Guideline 8 set out the information and documentation that needs to be provided for governance arrangements and internal controls.

3.~~63~~62 We will assess if the applicant's 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 and use of branches, agents and distributors
- volume and size of its transactions
- degree of risk associated with each area of its operation

3.~~64~~63 Paragraphs 5 to 12 of Schedule 2 of the PSRs 2017 and paragraphs 5 to 7 of Schedule 1 of the EMRs set out information requirements that are relevant to these conditions, and more detail is provided in the Guidelines.

~~**Governance and internal control controls (paragraph 5 Schedule 2 PSRs 2017 and paragraph 5 Schedule 1 EMRs**~~

~~**3.65** API Guideline 8 and EMI Guideline 8 set out the information and documentation that needs to be provided for governance arrangements and internal controls.~~

~~3.66~~64 Governance arrangements are the procedures used in the decision-making and control of the business that provide its structure, direction and accountability.

3.~~67~~65 The description of control mechanisms must include a mapping of the risks identified by the applicant (including the types of risks), and the applicant should provide details of the procedures that it will put in place to assess and prevent such risks. These 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 applicant or its services might be used for a purpose connected with financial crime)

- foreign exchange risk (fluctuations in exchange rates)

3.~~68~~66 The risk management procedures provided in the application should show how the applicant will effectively identify, manage, monitor and report any risks to which it might be exposed. Depending on the nature and scale of the business and the payment services being undertaken, it may be appropriate for the applicant to operate an independent risk management function. Where this is not appropriate, the applicant should be able to demonstrate that the risk management policies and procedures it has adopted are effective.

3.~~69~~67 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 and EMRs in relation to its customers.

3.~~70~~68 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 and e-money activities that the applicant intends to carry on.

Security incident and security-related customer complaint procedures (paragraph 6 Schedule 2 of the PSRs 2017 and paragraph 5A Schedule 2 of the EMRs)

3.~~71~~69 API Guideline 9 and EMI Guideline 9 set out the information and documentation required with respect to procedures for monitoring, handling and following up security incidents and security-related customer complaints. The information required should include details of how the applicant will comply with its obligation to report major operational or security incidents under regulation 99 of the PSRs 2017 – see **Chapter 13 – Reporting and notifications** for more information on the incident reporting ~~requirements.~~
Requirements and EBA Guidelines on major incident reporting.[13]

3.~~72~~70 Applicants should provide a description of the procedures in place to monitor, handle and follow up on security incidents and security-related customer complaints including the individuals and bodies responsible for assisting customers in the cases of fraud, technical issues and/or claim management. The applicant's complaints procedures must demonstrate compliance with regulation 101 of the PSRs 2017 for non-eligible complainants and our Dispute Resolution Sourcebook (DISP) for eligible complainants. See **Chapter 11 – Complaints handling**.

Sensitive payment data processes (paragraph 7 Schedule 2 of the PSRs 2017 and paragraph 5B Schedule 2 of the EMRs)

3.~~73~~71 API Guideline 10 and EMI Guideline 10 set out the information and documentation which is required in relation to the applicant's processes to file, monitor, track and restrict access to sensitive payment data. See also **Chapter 18 – Operational and security risks**.

13 http://www.eba.europa.eu/documents/10180/1914076191FINAL/Guidelines+on+incident+reporting+under+PSD2+%28EBA-GL-2017-10%29.pdf/3902c3db-c86d-40b7-b875-dd50eec87657

Business continuity arrangements (paragraph 8 of Schedule 2 of the PSRs 2017 and paragraph 5C Schedule 1 of the EMRs)

3.~~74~~72 API Guideline 11 and EMI Guideline 11 set out the information and documentation which is required in relation to the applicant's business continuity arrangements.

3.~~75~~73 Applicants must provide their business continuity and disaster recovery plans which should include failure of key systems, the loss of key data, inaccessibility of premises and loss of key persons.

The principles and definitions used by the applicant in collecting statistical data on performance, transactions and fraud (paragraph 9 of Schedule 2 PSRs 2017 and paragraph 5D of Schedule 1 EMRs)

3.~~76~~74 API Guideline 12 and EMI Guideline 12 set out the information and documentation required in relation to the collection of statistical data on performance, transactions and fraud. This should demonstrate how the applicant will ensure it can meet its obligation to report to us on fraud (see **Chapter 13 – Reporting~~ and notifications~~**).

Security policy (paragraph 10 Schedule 2 of the PSRs 2017 and paragraph 5E Schedule 1 of the EMRs)

3.~~77~~75 API Guideline 13 and EMI Guideline 13 set out the information and documentation which is required in relation to the applicant's security policy. The security policy must include a detailed risk assessment of the services to be provided (including-
risks of fraud) and the mitigation measures to protect users from the risks identified. It must also describe how applicants will maintain the security of e-money and payment processes, including customer authentication procedures (see **Chapter 20 – Authentication**). Applicants should additionally include a description of the IT systems and the security measures that govern access to these systems. As part of the information required under EBA Guideline 13.1 we would expect the security policy to take into account the security of data at rest and in transit. If the data is held off-site by a third party, we would expect details on how it is encrypted and regular due diligence carried out.

3.~~78~~76 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). Applicants may wish to consider the use of security training, accreditation and/or certification to support their application (in particular government-backed schemes, e.g. Cyber Essentials, a security certification scheme that sets out a baseline of cyber security for organisations).~~10~~
14

3.~~79~~77 More information on security can be found in **Chapter 18 – Operational and security risks**.

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

3.~~80~~78 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 (MLRs) and the EU Funds Transfer Regulation (EU 2015/847).

14 https://www.cyberaware.gov.uk/cyberessentials/

3.~~81~~ 79 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.~~82~~80 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 ensuring compliance with anti-money laundering and ~~counter-~~ counterterrorism obligations is clearly allocated (see also Governance arrangements and risk management controls at paragraph 3.~~159~~157).

3.~~83~~ 81 As part of the information provided by applicants, and in accordance with the MLRs, we expect details on the risk-sensitive anti-money laundering policies, procedures and internal controls related to:

- customer due diligence checks

~~10 https://www.cyberaware.gov.uk/cyberessentials/~~

- 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.~~84~~82 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.~~85~~83 Applicants must also provide us with the name of the person (the Money Laundering Reporting Officer) nominated to receive disclosures under Part 7 of the Proceeds of Crime Act 2002 and referred to in regulation 21(3) of the MLRs. Where different, applicants must also provide us with the name of the individual appointed under regulation 21(7) of the MLRs.

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

3.~~86~~84 Applicants that are required to be registered with Her ~~Majesty's~~Majesty's Revenue and Customs (HMRC) under the MLRs will either need to be registered before we can

authorise them, or need to provide evidence that they have submitted the appropriate application to HMRC. This will apply to:

- most money service businesses (MSBs)
- bill ~~PSPs~~
  payment service providers
- telecommunication~~s~~, digital and IT PSPs

3.~~87~~85 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~~the applicant should provide their application~~, but cannot grant authorisation until the MLR registration number has been received~~.

3.~~88~~86 We will verify with HMRC that the registration or application number provided to us matches a valid ~~MLR registration~~ MLR registration or application for that firm.

3.~~89~~87 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.

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

3.~~90~~88 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 af fairs of the applicant. This comprises two elements: first, the applicant will need to assess whether any persons (or entities) have a qualifying holding in the applicant and notify us of their identity; and secondly, we will assess the fitness and propriety of any such persons (or entities).

Assessment of qualifying holdings

3.~~91~~89 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.~~92~~90 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); or
- is able to exercise significant influence over the management of the applicant firm through their voting power in it or a parent.

3.~~93~~91 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). One of the members may still, however, 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.~~94~~92 API Guideline 15 and EMI Guideline 15 set out all the information and documentation which must be provided in relation to qualifying holdings in PIs and EMIs. For each qualifying holding in the applicant, an authorisation ~~application must contain the following information~~applicant must provide:

- information relating to 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 or EMI (as applicable)

3.~~95~~ ~~API Guideline 15 and EMI Guideline 15 set out the~~ **93** The relevant forms for providing this information ~~and documentation which must be provided in relation~~are available via Connect. We attach considerable importance to ~~qualifying holdings in PIs and EMIs. Applicants should provide this in~~ the completeness and accuracy of the ~~PI or EMI~~ 'Qualifying ~~Holdings~~Holding' form. If the applicant is in any doubt as to whether or not any information is relevant, it should be included.

Assessment of suitability of controllers

3.~~96~~94 The term 'fit and proper' is used frequently in the context of individuals approved under FSMA. We have interpreted this term, which is used in regulation 6 of the PSRs 2017 and regulation 6 of the EMRs in relation to controllers, to mean in substance the same for PIs and EMIs as it does for individuals approved in FSMA firms, subject to differences introduced by the EBA Guidelines. 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, as well as the EBA Guidelines, helpful.

3.~~97~~95 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 'fit~~ness~~ and ~~propriety~~'proper', which is used in regulation 6 of the PSRs 2017 and regulation 6 of the EMRs. Although these terms are different, they incorporate the same essential factors, namely the:

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

of the person with a qualifying holding, having regard to the need to ensure the sound and prudent management of a PI or EMI (as applicable).

~~**3.98** Whilst it is impossible to list every fact or matter~~For more detail on our assessment of controllers' fitness and propriety, see section 3.101 'Assessing fitness and propriety'.

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

3.96 The applicant must satisfy us that ~~would~~ its directors and any other persons who are or will be responsible for the management of the applicant 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.

3.97 This incorporates two elements: first, identification by the applicant of those with responsibility for the payment service or e-money activities of the applicant. 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 Individual or EMD Individual, must provide full and complete information to us about all PSD Individuals 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 set out the information and documentation required in relation to the identity and suitability of directors and persons responsible for the management of the applicant. Please see our webpages for the notes and the factsheet to completing the PSD Individual form or EMD Individual form. 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.

Identification of those with responsibility for the payment service or e-money activities of the applicant

3.98 In the case of an applicant 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 Individual or EMD Individual forms for each and every manager of the applicant, 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. However, examples of directors and persons likely to be responsible for payment services or e-money issuance (in addition to directors with qualifying holdings as discussed above) include, but are not limited to:

- persons within the payment or e-money institution that are responsible for each of the outsourced activities
- persons responsible for the internal control functions (including for periodic, permanent and compliance control) e.g. Compliance Officer
- persons in charge of ensuring the applicant's compliance with anti-money laundering and counter-terrorism obligations e.g. MLRO.

3.99 In the case of applicants 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 Individual or EMD Individual forms only for those Directors and persons with responsibility for running the firm's payment services activities and e-money issuance activities.

Assessment of good repute, knowledge and experience of identified individuals

3.100 We consider the term 'of good repute' to include the same essential factors relating to fitness and propriety set out below in relation to controllers. This means that we will consider the same essential factors set out in paragraph 3.95 above (and described in the next section) in respect of all directors and all individuals who are or who will be responsible for the management of the PI or EMI or its payment services and/or e-money issuance activities.

Assessing fitness and propriety

3.101 We will assess the fitness and propriety of a controller, or an individual on the information provided in the application form, including PSD or EMD Individual forms 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 investigations. Additionally, we require the disclosure of all spent and unspent criminal convictions and cautions (other than those criminal convictions and cautions that are protected).[15]

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

3.103 Examples of the matters we will consider for each factor are set out below. It is not possible, however, to list all the matters that would be relevant to a particular controller or individual.

Honesty, integrity and reputation

3.104 In determining the honesty, integrity and reputation of a controller or an individual, the following are examples of factors that we will consider. Whether:

- an assessment of the reputation of the controller or individual has already been conducted by a competent authority;

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

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

- 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;

15 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.

- the person has been the subject 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.);

- 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;

- 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;

- the person has been subject to relevant disciplinary action (including disqualification as company director);

- in the past, the person has been candid and truthful in all their 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.

~~**3.99** 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 of the PSRs 2017, regulation 6(6)(b) and paragraph 9, Schedule 1 of the EMRs)**~~

~~**3.100** The applicant must satisfy us that its directors and any other persons who are or will be responsible for the management of the applicant 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.~~

~~**3.101** This incorporates two elements: first, identification by the applicant of those with responsibility for the payment service or e-money activities of the applicant. 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 Individual or EMD Individual, must provide full and complete information to us about all PSD Individuals 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 set out the information and documentation required in relation to the identity and suitability of directors and persons responsible for the management of the applicant.~~

~~**3.102** In the case of an applicant 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 Individual or EMD Individual forms for each and every manager of the applicant, 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 applicants 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 Individual or 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~~

~~**3.103** 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 investigations. Additionally, we require the disclosure of all spent and

~~unspent criminal convictions and cautions (other than those criminal convictions and cautions that are protected).[11] 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.~~

~~**3.104** 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 3.98 above in respect of all directors and all persons who are or who will be responsible for the management of the PI or EMI or its payment services and/or e-money issuance activities.~~

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

~~**3.106** Examples of the matters we will consider for each factor are set out below. It is not possible, however, to list all the matters that would be relevant to a particular application or individual.~~

~~**Honesty, integrity and reputation**~~

~~**3.107** 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; and;~~
- ~~whether an assessment of the reputation of the individual has already been conducted by a competent authority.~~

~~**3.108** We will consider matters that may have arisen in the UK or elsewhere.~~

3.~~109~~ 106 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.~~110~~ 107 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 controller's or 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 controller or individual, the relevance of the offence to the proposed role, the passage of time since the offence was committed and evidence of the controller's or individual's rehabilitation.

~~11 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.~~111~~ 108 If a firm is not sure whether something may have an impact on a controller's or an individual's fitness and propriety, the information should be disclosed. We take the non-disclosure of material facts very seriously as it is seen as evidence of current dishonesty. If in doubt, disclose.

Competence, capability and experience

3.~~112~~109 In determining a controller's or 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 (only relevant for assessment of controllers)

3.110 In determining the suitability of a controller we will take into account a controller's financial soundness and we will consider any factors including, but not limited to:

- whether the controller has been the subject of any judgement, debt or award in the UK or elsewhere, that remains outstanding or was not satisfied within a reasonable period; or

- whether the controller 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.

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

3.~~113~~111 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 paragraph 3.~~42~~40 above.

3.~~114~~112 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 (e.g. a supervisory board in a two-tier board structure or non-executive committee in a one-tier structure)

3.~~115~~113 As well as any internal audit function, API Guideline 17 and EMI Guideline 17 require APIs and EMIs to provide information on the identity of its statutory auditor or audit firm.

Part II: Becoming a small PI or a small EMI

3.~~116~~114 Businesses can apply for registration as a small PI and be exempt from the authorisation and prudential requirements of the PSRs 2017 if they:

- do not intend to provide payment services on a cross-border basis or in another EEA State;
- have an average monthly payment value of not more than €3 million over the period of twelve months preceding their application (or, where the applicant has yet to commence payment services, or has been providing payment services for less than 12 months, the monthly average may be based on the projected total amount of payment transactions over a 12 month period); and
- do not intend to carry on AIS or PIS.

3.~~117~~115 Businesses can apply for registration as a small EMI and be exempt from the authorisation and prudential requirements of the EMRs if:

- they do not intend to provide payment services on a cross-border basis or in another EEA State;
- their total business activities are projected to generate average outstanding e-money that does not exceed €5 million;
- their monthly average turnover in respect of relevant unrelated payment service transactions over the period of 12 months preceding the application does not exceed €3 million (or, where the applicant has yet to commence the provision of payment services which are not related to the issuance of e-money, or has been providing such payment services for less than 12 months, the monthly average may be based on the projected total amount of the relevant transactions over a 12 month period); and
- they do not intend to carry out AIS or PIS.

3.~~118~~116 The conditions that must be met in order to become a registered small PI or small EMI are set out in regulation 14 of the PSRs 2017 and regulation 13 of the EMRs respectively. We provide guidance in relation to each of the conditions, and the associated information which we will request to assess these conditions, below. We also set out other information that applicants will need to provide when applying for registration.

Making an application

3.~~119~~117 Applicants to become a small PI or small EMI must pay a fee (see **Chapter 15 – Fees** for more information). No work will be done on processing an application until the full fee is received. The fee is non-refundable.

3.~~120~~118 For small PIs and small EMIs, 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 (small PIs only)	The sole trader
Partnership (small PIs only)	Two partners
Unincorporated association (not a limited partnership) (small PIs only)	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 – both small PIs and small EMIs

3.~~121~~119 We may refuse to register an applicant as a small PI or small EMI if any of the conditions specified in regulation 14 of the PSRs 2017 or regulation 13 of the EMRs (as applicable) have not been met. We provide guidance on the information which we will request from applicants below, including references to the PSRs 2017 or EMRs where relevant. This information will be requested from both small PIs and small EMIs.

Value of payment transactions – regulation 14(3) of the PSRs 2017 and regulation 13(4) of the EMRs

3.~~122~~120 To be eligible for registration as a small PI, the average monthly value of payment transactions (or, where applicable, projected monthly average) carried out by the applicant (including by agents on its behalf) must not exceed €3 million. In their application for registration, applicants will be required to self-certify that the business will meet the monthly value of payment transactions condition. If, however, we suspect that this might not be the case, we may ask for projected financial statements. We also ask the applicant to describe how it will monitor the monthly average value of payment transactions once it is registered. We expect applicants to have a clear and established process for monitoring this so that they know if the requirement to become authorised (monthly average payment transactions value exceeding €3 million) is triggered.

3.~~123~~121 For small EMIs, if the business plans to undertake payment services not connected with the issuing of e-money (unrelated payment services), then the monthly average of relevant payment transactions (or, where applicable, projected monthly average) must not exceed €3m. To register as a small EMI, an applicant must also not have total business activities that generate (or, where applicable, are projected to generate) average outstanding e-money that exceeds €5m. Small EMIs are required to provide-
financial forecasts with their business plans and more detail is provided below.

3.~~124~~122 Applicants will need to take account of changes in exchange rates where they

carry out.

transactions in different currencies. In our view, it would be reasonable for applicants

to use the Commission's monthly accounting rate of the euro (which is available on the InforEuro website) to calculate turnover in euro for a particular calendar month.~~12~~16

Business must not include the provision of account information services or payment initiation services – regulation 14(4) of the PSRs 2017 and regulation 13(4A) of the EMRs

3.~~125~~123 Small PIs and small EMIs are not permitted to carry out AIS or PIS. Businesses that wish to carry out these services will need to apply for authorisation or, in the case of a business only wishing to provide AIS, the business will need to apply to become a RAISP and cease providing other payment services or issuing e-money.

Convictions by management – regulation 14(5) of the PSRs 2017 and regulation 13(8) of the EMRs

3.~~126~~124 None of the individuals responsible for the management or operation of the applicant can have been convicted of offences relating to money laundering, terrorist financing or other financial crimes. We will ask the applicant to confirm on the application form that this is the case.

3.~~127~~125 Financial crime includes fraud or dishonesty, offences under FSMA, the PSRs 2017 or the EMRs, and acts or omissions that would be an offence if they took place in the UK. We require the disclosure of spent and unspent criminal convictions and cautions unless the relevant conviction or caution is protected.

Qualifying holdings – regulation 14(6) of the PSRs 2017 and regulation 12(1) paragraph 4 of Schedule 3 of the EMRs

3.~~128~~126 Where the applicant is a partnership, an unincorporated association or a body corporate, it must provide evidence that any persons having a qualifying ~~holding~~[13] holding[17] in it (a 'controller') are suitable having regard to the need to ensure the sound and prudent conduct of the affairs of the small PI or small EMI. For small PIs, the applicant must satisfy us that any controller is fit and proper.

3.~~129~~127 The information that we will require about qualifying holdings for an application for registration as a small PI ~~and small EMI~~ is the same as for an application for authorisation as an authorised PI ~~and authorised EMI~~ (set out in Part I above~~). Small~~) and small PIs will need to submit controller forms for persons with a qualifying holding. Small EMIs will need to identify their controllers in the application form but are not required to submit separate forms for persons with a qualifying holding.

Directors, managers and persons responsible for payment services – regulation 14(7) of the PSRs 2017 and regulation 13(7)(a) of the EMRs

3.~~130~~128 The requirements for the directors, managers and persons responsible for the management of e-money and/or payment services (as applicable) of the small PI or small EMI are the same as those for an authorised PI or authorised EMI. We will take the same approach to assessment of individuals as set out in Part I above. This includes applying the same 'fitness and propriety' test described above (section 3.101).

16 http://ec.europa.eu/budget/contracts_grants/info_contracts/inforeuro/index_en.cfm

17 'Qualifying holding' is defined by Regulation (EU) 575/2013 (Capital Requirements Regulation) as a direct or indirect holding in an undertaking which represents 10 % or more of the capital or of the voting rights or which makes it possible to exercise a significant influence over the management of that undertaking.

Close links – regulation 14(8) of the PSRs 2017 and regulation 12(1) of the EMRs

3.~~131~~129 For applicants that are bodies corporate the information we will require about 'close links' for applications as a small PI or small EMI is the same as those for an authorised PI (see Part I above).

~~12 http://ec.europa.eu/budget/contracts_grants/info_contracts/inforeuro/index_en.cfm~~

~~13 'Qualifying holding' is defined by Regulation (EU) 575/2013 (Capital Requirements Regulation) as a direct or indirect holding in an undertaking which represents 10 % or more of the capital or of the voting rights or which makes it possible to exercise a significant influence over the management of that undertaking.~~

Location of head office, registered office or place of residence – regulation 14(10) of the PSRs and regulation 13(9) of the EMRs

3.~~132~~130 For applicants to be either a small PI or a small EMI, their head office, registered office or place of residence, as the case may be, must be in the UK.

3.~~133~~131 Only bodies corporate (e.g. a limited company or Limited Liability Partnership (LLP)) can apply to become a small EMI. An applicant to become a small PI may be a natural person, in which case their place of residence must be in the UK.

3.~~134~~132 The location of the head office, registered office and principal place of business is to be supplied as part of the contact details. ~~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~~In assessing the location of ~~its central management and control, that is, the location of:~~

~~**1.** 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; and~~

~~**2.** the central administrative functions of the firm (e.g. central compliance, internal audit).~~

the head office, we will take the approach set out in section 3.~~**135** For the purpose of regulation 14(10) of the PSRs 2017 and regulation 13(9) of the EMRs, a 'virtual office' in the UK does not satisfy this condition. If the applicant to become a small PI is a natural person their place of residence must be in the UK~~49– 3.53 above.

Money Laundering ~~Registration~~registration – regulation 14(11) of the PSRs 2017 and regulation 13(10) of the EMRs

3.~~136~~133 The applicant must comply with the registration requirements of the MLRs, where those requirements apply to it (see 3.~~86~~84-3.~~89~~87 in Part I above for more on MLR registration requirements).

3.~~137~~134 Where we will be responsible for money laundering supervision of the applicant, no separate registration is required. This will be the case for all small 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 'Small Payment Institution' or 'Small E-money Institution' form, as these combine both MLR registration and PSRs 2017/EMR ~~authorisation~~registration.

3.~~138~~135 Applicants are required to provide a description of the anti-money laundering policies, procedures and controls in place.

Programme of operations

3.~~139~~136 Applicants to become small PIs and small EMIs will need to provide a description of their main business and the payment services envisaged, including an explanation of how the activities and the operations fit into the list of payment services set out in Part 1 of Schedule 1 of 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 3 and Chapter 15 of PERG.

Security incidents and customer complaints

3.~~140~~137 For small PIs and small EMIs, the information required in the registration application includes details of how the applicant will comply with its obligation to report major operational or security incidents under regulation 99 of the PSRs 2017 – see **Chapter 13 – Reporting and** ~~our~~**notifications** for more information on the incident reporting ~~Handbook~~requirements.

3.~~141~~138 Applicants will also need to describe the complaints procedures in place for customers that comply with regulation 101 of the PSRs 2017 for non-eligible complainants and
our Dispute Resolution Sourcebook (DISP) for eligible complainants. See **Chapter 11 – Complaints handling**.

3.139 The requirements for reporting of security incidents and customer complaints expected for small PIs or small EMIs are the same as those for an authorised PI or authorised EMI (see Part I above).

Sensitive payment data

3.~~142~~140 For small PIs and small EMIs, the application form requests a description of the applicant's process to file, monitor, track and restrict access to sensitive payment data. The requirements for handling sensitive payment data expected for small PIs or small EMIs are the same as those for an authorised PI or authorised EMI (see Part I above).

Statistical data on performance, transactions and fraud

3.~~143~~141 For small PIs and small EMIs, applicants are required to provide a description of the procedures they have in place for collecting statistical data on fraud (including the means of collecting collected). This should demonstrate how the applicant will ensure it can meet its obligations to report to us (see **Chapter 13 – Reporting and notifications**).

Security policy

3.~~144~~142 Applicants will need to provide a description of their security policy which 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. 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). They may wish to consider the use of security training, accreditation and/or certification to support their application (in particular government-backed schemes, e.g. Cyber Essentials, a security certification scheme that sets out a baseline of cyber security for organisations).[~~14~~18] For small PIs and small EMIs, applicants must provide a description of the key IT systems in use which will support the provision of payment services, including off-the-shelf and bespoke packages. Applicants will also need to confirm whether they are already using these systems. The requirements for security expected for small PIs or small EMIs are the same as those for an authorised PI or authorised EMI (see Part I above) and include the physical security of applicants' premises.

3.~~145~~143 As small EMIs are inherently reliant on IT systems to ensure they operate soundly, we intend to assess IT systems during the approval process. Applicants must satisfy us that their overall IT strategy is proportionate to the nature, scale, and complexity of the business and is sufficiently robust to facilitate, on an ongoing basis, their compliance with the conditions of registration.

Safeguarding

Small EMIs – regulation 13(7)(c) EMRs

3.~~146~~144 Small EMIs are subject to the same safeguarding obligations with respect to funds that have been received in exchange for e-money as authorised EMIs, and the information that we require is the same (please refer to the information on safeguarding for authorised EMIs in Part I above).

~~14~~

18 https://www.cyberaware.gov.uk/cyberessentials/

3.~~147~~145 Small EMIs that provide unrelated payment services may choose to safeguard funds received for the execution of payment transactions that are not related to the issuance of e-money. Where they choose to comply, the requirements are the same as those for an authorised EMI or authorised PI (please refer to the information on safeguarding for authorised EMIs in Part I above).

Small PIs

3.~~148~~146 Small PIs can choose to comply with safeguarding requirements in order to offer the same protections over customer funds as authorised PIs must provide. Where they choose to comply, the requirements are the same as those for an authorised PI (please refer to the information on safeguarding for authorised PIs in Part I above).

3.~~149~~147 There is more information on safeguarding in **Chapter 10 – Safeguarding**, including guidance on what we would expect to see by way of organisational arrangements.

~~Information~~Additional information to be provided and conditions of registration – small EMIs only

3.~~150~~148 There are conditions of registration set out in regulation 13 of the EMRs which must be met by small EMIs but do not apply to small PIs. Below we set out information we will only request from applicants to become small EMIs.

Business plan – regulation 13(7)(b) of the EMRs

3.~~151~~149 The business plan has 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.~~152~~150 The plan must include a forecast budget for the first three financial years. The budget has to demonstrate that the applicant is able to employ appropriate and proportionate systems, resources and procedures to operate soundly, and that it will be able to continue to meet the initial capital requirements and the ongoing capital (own funds) requirement, if applicable.

3.~~153~~151 The business plan should also include, but not be limited to, the following:

- background to the application;
- a description of the e-money issuance and payment services business (this should include a step-by-step description from start to end of how the e-money will be issued by the applicant and redeemed by the customer);
- sources of funding;
- target markets; and

- a marketing plan.

3.~~154~~152 If the applicant intends to provide unrelated payment services then a separate business plan for these, covering the information required above, should also be submitted.

Initial capital – regulation 13(5) EMRs

3.~~155~~153 By the time of registration, the applicant must provide evidence that it holds initial capital at the level required by Part 1 of Schedule 2 of the EMRs. The level of initial capital required varies according to the average value of outstanding e-money:

- where the business activities of an applicant generate average outstanding e-money of €500,000 or more, the capital requirement is at least equal to 2% of the average outstanding e-money of the institution; and
- where the business activities of an applicant generate average outstanding e-money of less than €500,000, there is no capital requirement.

3.~~156~~154 Where an applicant to become a small EMI has not completed a sufficiently long period of business to compile historical data adequate to make that assessment, the applicant must make the assessment on the basis of projected outstanding e-money as evidenced by its business plan, subject to any adjustments to that plan required by us.

3.~~157~~155 The evidence that should be provided will depend on the type of business and its source of funding. For example, if an applicant is 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 last year-end accounts may be sufficient (or interim accounts if appropriate). Businesses may wish to capitalise nearer to the time of registration, so this evidence can be provided at a later date, but it will be required before registration is granted. For an application to be complete we must be satisfied that the initial capital will be in place immediately before registration.

3.~~158~~156 Small EMIs that are required by the EMRs to hold initial capital are also required to maintain adequate own funds on an ongoing basis, by reference to paragraph 14 of Schedule 2 of the EMRs. See **Chapter 9 – Capital resources and requirements** for more information.

Governance arrangements and risk management controls – regulation 13(6) EMRs

3.~~159~~157 Applicants to become a small EMI are required to provide descriptions of the governance arrangements and risk management procedures they will use when issuing e-money and providing payment services. We will assess whether the arrangements, controls and procedures are appropriate, sound and adequate, taking into account a number of factors, such as the:

- types of payment services and e-money envisaged;
- nature, scale and complexity of the business;
- diversity of its operations, including geographical diversity;
- volume and size of its transactions; and
- degree of risk associated with each area of its operations.

~~Governance arrangements~~

3.~~160~~158 Governance arrangements are the procedures used in the decision-making and control of the business that provide its structure, direction and accountability.

3.~~161~~159 The description of the governance arrangements must include a clear organisational structure with well-defined, transparent and consistent lines of responsibility (regulation 13(6)(a) of the EMRs). If applicable, this should cover the unrelated payment services business as well as the e-money business. We would also expect to receive information on:

- decision-making procedures;
- accounting procedures for monitoring that the average outstanding e-money and payment services transactions do not exceed the thresholds for authorisation (see paragraphs 3.~~124~~120-3.122);
- reporting lines;
- internal reporting and communication processes;
- the arrangements for regular monitoring of internal controls and procedures; and
- measures that would be taken to address any deficiencies.

Risk management

3.~~162~~160 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 (regulation 13(6)(b) of the EMRs). Such risks may include risks in relation to both the e-money business and any payment services business:

- settlement risk (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 EMI or its services might be used for a purpose connected with financial crime); and
- foreign exchange risk (fluctuation in exchange rates).

~~3.163~~

Depending on the nature and scale of the business and any payment services being provided, it may be appropriate for the small EMI to operate an independent risk management function. Where this is not appropriate, the small EMI should nevertheless be able to demonstrate that the risk management policies and procedures it will adopt are effective.

Part III: Becoming a RAISP

3.~~164~~161 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 of the PSRs 2017.

3.~~165~~162 RAISPs may not provide any payment services other than AIS.

3.~~166~~163 Applicants to become RAISPs must pay a fee (see **Chapter 15 – Fees** for more information). No work will be done on processing an application until the full fee is received. The fee is non-refundable.

3.~~167~~164 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
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.~~168~~165 We may refuse to register an applicant as a RAISP if the conditions in regulation 18 of the PSRs 2017 are not met. This includes where, if registered, the grounds in regulation 10 of the PSRs 2017 (cancellation of authorisation) as applied by regulation 19 of the PSRs 2017 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 an application.

3.~~169~~166 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 1 of PSD2 (account information services)) of the EBA Guidelines (the RAISP Guidelines).[19] Together, these documents explain the information that must be supplied with the application and the conditions that must be satisfied.

19 https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-authorisation-and-

registration-under-psd2

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

3.~~170~~167 The information and documentation which needs to be provided in the programme of operations for RAISP applications is set out in RAISP Guideline 3. These are similar to those for an authorised PI (see Part I).

3.~~171~~168 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 the applicant's name, funds in an account in the applicant's name at another PI and funds held on trust for the applicant.

3.~~172~~169 The applicant is also required to provide copies of draft contracts between all parties involved, and terms and conditions of the provision of the AIS. We would expect this information to cover the nature of the service being provided to the customer, how their data will be used, and how the applicant will obtain appropriate consent(s) from the customer. See **Chapter 17 – Payment initiation and account information services and confirmation of availability of funds** for more information.

Business plan (paragraph 2, Schedule 2 of the PSRs 2017)

3.~~173~~170 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). This should ~~include how~~contain a forecast budget calculation for the ~~user of customer data fits into~~first ~~the applicant's business model~~3 years .

Structural organisation (Paragraph 12 of Schedule 2 of the PSRs 2017)

3.~~174~~171 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. This should include details of outsourcing arrangements, as RAISPs will need to demonstrate that these arrangements allow them to fulfil the conditions of registration. These are similar to those for an authorised PI (see Part I).

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

3.~~175~~172 The governance arrangements, internal controls and risk management requirements for applications as RAISPs are outlined in RAISP Guideline 6. ~~Governance arrangements~~These are ~~the procedures used in the decision-making and control of the business that provide its structure, direction and accountability.~~

~~**3.176** 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~~similar to ~~which the applicant might be exposed.~~those

~~**3.177** 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 (RAISP) or its services might be used~~ for ~~a purpose connected with financial crime)~~

an authorised PI (see Part I).

- ~~foreign exchange risk (fluctuations in exchange rates)~~

3.~~178~~173 Depending on the nature, scope and ~~scale~~complexity 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 – Operational and security risks**.

~~**3.179** 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 of the PSRs 2017)

3.~~180~~174 The information and documentation which needs to be provided for security incidents and security-related customer complaints requirements for applications as RAISPs are set out in RAISP Guideline 7~~ see **Chapter 11 – Complaint handling**~~. These are similar to those for ~~complaints~~an authorised PI (see Part I). ~~handling requirements that apply RAISPs. The information required includes details of how the applicant will comply with its obligation to report major operational or security incidents under regulation 99 of the PSRs 2017. See **Chapter 13 – Reporting and notifications** for more information on the incident reporting requirements.~~

~~**3.181** Applicants should provide a description of the procedures in place to monitor, handle and follow up on security incidents and security related customer complaints including the individuals and bodies responsible for assisting customers in the case of fraud, technical issues and/or claim management.~~

Sensitive payment data (paragraph 7, Schedule 2 of the PSRs 2017)

3.~~182~~175 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. These are similar to those for an authorised PI (see Part I). See also **Chapter 18 – Operational and security risks**.

Business continuity arrangements (paragraph 8, Schedule 2 of the PSRs 2017).

3.~~183~~176 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.~~

~~**3.184** Applicants must provide their business continuity and disaster recovery plans which should include the failure of key systems, loss of key data, inaccessibility of premises and loss of key persons.~~

Guideline 9. These are similar to those for an authorised PI (see Part I).

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

3.~~185~~177 The information that should be provided in a security policy document is set out in RAISP Guideline 10. ~~The security policy must include a detailed risk assessment in relation~~These are similar to ~~the services to be provided, including risks of fraud 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. It must also describe how applicants will maintain the security of payment services processes, including customer authentication procedures. Applicants should additionally include a description of the IT systems and the security measures that govern access to these systems.~~

~~**3.186** 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). Applicants may wish to consider the use of security training, accreditation and/or certification to support their application (in particular government-backed schemes, e.g. Cyber Essentials, a security certification scheme that sets out a baseline of cyber security~~those for ~~organisations).~~[15]

~~**3.187** More information on security can be found in **Chapter 18 – Operational and security risks**~~an authorised PI (see Part I).

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

3.~~188~~178 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.

3.~~189~~179 PSD Individual forms should be provided as set out in Part I for authorised PIs. In assessing whether the information relating to directors and managers indicates that that the conditions in regulation 18 of the PSRs 2017 are met (e.g. registration would not be contrary to the interests of consumers) we will take a similar approach to that we take to assess the fitness and propriety of directors and persons responsible for the management of authorised PIs and EMIs (see ~~paragraphs 3.103 to 3.112~~Part I above).

Audit arrangements (Paragraph 18 of Schedule 2 of the PSRs 2017)

3.~~190~~180 RAISP Guideline 6 requires that an applicant provides the identity of any auditor that is not a statutory auditor.

3.~~191~~181 Paragraph 18 of Schedule 2 of the 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 of the PSRs 2017)

3.~~192~~182 The applicant must satisfy us that it holds appropriate PII or a comparable guarantee. RAISP Guideline 12 sets out the information and documentation which is required in relation to this PII or comparable guarantee. The required PII or comparable guarantee must meet or exceed the minimum monetary amount directed by us from time to

time. This direction has been made in paragraph 3.61.

15 https://www.cyberaware.gov.uk/cyberessentials/

time. This direction has been made in paragraph 3.59.

Address of the head office (paragraph 17, Schedule 2 of the PSRs 2017)

3.183 The applicant must provide the address of its head office. There is no requirement in the PSRs 2017 for this to be in the UK although we must be able to effectively supervise the applicant once it is registered. We will judge each application on a

case-by-case basis. As above, we may refuse to register an applicant as a RAISP if any of the conditions in regulation 18(1) of the PSRs 2017 applies. One of those conditions is that, if the applicant were registered, there would be grounds for cancellation (under regulation 10, as applied by regulation 19 of the PSRs 2017).

Part IV: Decision-making process

3.~~193~~184 This section relates to the decision-making process for all applications for authorisation and registration under the PSRs 2017 and the EMRs.

3.~~194~~185 Having assessed the application and all the information provided, we will make a decision to either approve or reject it. This decision will be notified to the applicant, along with instructions for the appeal process, if relevant.

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

3.~~195~~186 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 and when your application becomes complete.

3.~~196~~187 Our commitment[20] to dealing with applications for authorisation or registration are as follows:

- We will tell you that we have received your application within 3 working days
- We will contact you again within 3 weeks, normally to tell you which case officer we have assigned to your application or to tell you the date by which we will assign your application. The assigned case officer will handle all communication about your application. We will also give you an alternative person to contact if your assigned case officer is unavailable.
- If we subsequently have to assign your case to a different case officer, we will tell you this within 3 working days of making the change and give you the new contact details.
- We will acknowledge all communications from you within 2 working days.
- We will usually give you a substantive response within 10 working days. If this is not possible, we will send you an update within the 10-working day period to tell you when you should expect to receive a substantive response.
- We will give you clear deadlines when we ask you to send us additional information.
- The designated case officer will give you an update on the current status of your case at least monthly and often more frequently.

20 https://www.fca.org.uk/publication/corporate/our-approach-authorisation.pdf p. 21

These commitments will apply until we approve your application or tell you of our decision that it should be refused, in which case we will apply the formal refusal process.

3.188 In the case of an incomplete application, we must make a decision within 12 months of receipt. If discussions with the applicant have not resulted in us receiving all the information we need within that 12-month period so that the application is incomplete it is likely that the application will be refused. This is because it is unlikely we will have been able to satisfy ourselves that the applicant has met the authorisation/registration requirements.

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

~~3.197~~ 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) of the PSRs 2017, regulation 9(4) and (5) of the ~~of the~~ EMRs)

3.~~198~~190 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.~~199~~191 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 of the PSRs 2017 and regulation 7 of the EMRs). This may include requiring the applicant to take a specified action or refrain from taking a specified action (e.g. 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.~~200~~192 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 applicant or its

20 https://www.fca.org.uk/publication/corporate/our-approach-authorisation.pdf p. 21

financial soundness, we can require the applicant to form a separate legal entity to issue the e-money and/or perform payment services.

3.~~201~~193 We will update the Financial Services Register as soon as possible after granting the authorisation or registration. The Financial Services Register will show the contact details of the business, 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) of the PSRs 2017, regulation 9(6) to (8) of the EMRs)

3.~~202~~194 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 them 28 days to make a representation on the decision.

3.~~203~~195 Applicants can make oral or written representations. If oral representations are required, we should be notified within two weeks of the warning notice, so that arrangements can be made for a meeting within the 28-day deadline.

3.~~204~~196 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 will then issue the final notice.

3.~~205~~197 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. We may not, however, 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 154 of the PSRs 2017, regulation 78A of the EMRs)

3.~~206~~198 In order to continue providing payment ser vices, PIs and EMIs authorised or registered under the PSRs 2009 or the EMRs must be re-authorised or re-registered. They must also pay a fee (see **Chapter 15 – Fees** for more information).

3.~~207~~199 Existing PIs and EMIs must comply with the new requirements of PSD2 (introduced through the PSRs 2017 and our Handbook), including conduct of business changes, new complaints handling timeframes and new reporting and notifications from
13 January 2018, prior to becoming re-authorised or re-registered. Businesses should review the start date for each requirement as there are some exceptions, in particular in relation to changes in control.

3.~~208~~200 There are also transitional provisions for firms that have been providing AIS or PIS prior to 12 January 2016, which determine when they will need to get authorised or registered.

20 https://www.fca.org.uk/publication/corporate/our-approach-authorisation.pdf p. 21

~~Authorised PIs and small PIs~~

~~**3.209** An authorised PI must provide to us any 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 us that it has already been provided) before 13 April 2018 in order to continue providing payment services on or after 13 July 2018.~~

~~**3.210** We will treat this as an application for authorisation under the PSRs 2017, and assess it in accordance with the guidance set out in this chapter.~~

~~**3.211** 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).~~

~~**3.212** The application for registration under these provisions will be assessed in the normal way.~~

~~**3.213** 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 of the PSRs 2017 (prohibition on provision of payment services by persons other than PSPs).~~

Authorised EMIs ~~and Small EMIs~~

~~**3.214** An authorised EMI must provide to us any 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 us that it has already been provided) before 13 April 2018 in order to continue issuing e-money or providing payment services on or after 13 July 2018.~~

~~**3.215** A small EMI that intends to provide services on or after 13 July 2018 as a small EMI must notify us whether it continues to meet the requirements for registration, and provide any information relevant to meeting the requirements, before 13 April 2018.~~

~~**3.216** On receipt of this information we will consider whether the EMI's authorisation or registration should be continued after 13 July 2018. If we do not decide to continue the EMIs authorisation or registration it is treated as cancelled on 13 July 2018.~~

~~**3.217** Businesses which fall into all of 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.~~

~~**3.218** Application forms are available on the payment services section of our website.~~

~~**3.219**~~**201** Under regulation 78A(2)(b) of the 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.

Businesses providing AIS or PIS

3.~~220~~202 Businesses that started providing PIS or AIS on or after 12 January 2016 ~~will need~~had to be authorised to provide these services (or registered, if only providing AIS) by ~~13 January~~ 13 January 2018 to continue providing these services. For existing authorised ~~PIs~~ payment institutions this means that they will need to have successfully applied for re-authorisation and a variation to add AIS or PIS~~, for~~. For existing authorised EMIs, they ~~will need to have successfully applied~~ will need to have successfully applied for re-authorisation that permits them to provide AIS or PIS or for the requirement imposed by regulation 78A(2)(b) of the EMRs to be removed. ~~Businesses may apply to vary at the same time as they apply for re-authorisation.~~ Existing small PIs and small EMIs will have to cease providing these services, or become authorised.

3.~~221~~203 Providers of AIS and PIS which were providing those services before 12 January 2016 and which continue to provide such services immediately before 13 January 2018 will be able to continue to do so ~~after that date~~ until 14 September 2019 (when the Regulatory Technical Standards on strong customer authentication and secure communication (SCA-RTS) ~~apply.~~[16] come into effect).[21] This means:

- ~~Businesses~~

21 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN

- businesses that fall within the transitional provision and are not authorised or registered may continue to operate without authorisation or registration until ~~the SCA-RTS applies~~ 14 September 2019

- existing PIs and EMIs that fall within the transitional provision do not need to have obtained variation of their authorisation to add the appropriate permission/remove the requirement until ~~the SCA-RTS applies~~ 14 September 2019

- small PIs and small EMIs that fall within the transitional provision do not need to be authorised until ~~the SCA-RTS applies~~14 September 2019.

3.~~222~~204 We expect that businesses benefitting from this transitional provision will nonetheless apply to be authorised (or registered, if only providing AIS) or for variation of their authorisation ~~before the application of the SCA-RTS~~in good time before 14 September 2019. While providing AIS and PIS in reliance on the transitional provision, these businesses will not be considered PISPs or AISPs under the PSRs 2017. This means they will not have the entitlement to access payment service users' online payment accounts that PISPs and AISPs have (see **Chapter 17 – Payment initiation and account information services and confirmation of availability of funds**).

16 ~~The EBA has published final draft *Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of PSD2* (EBA/RTS/2017/02). The SCA-RTS will not come into force until they have been published in the EU's Official Journal, whereupon they will take effect as a Delegated Commission Regulation. We will review this Approach Document after the SCA-RTS have taken effect and update it as we deem necessary.~~

Payments through network operators

3.205 Where a PI provided payment services of the type described in paragraph 1(g) of Schedule 1 of 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 us before 13 January 2020 that it complies with relevant own funds requirements.

~~**Payments through network operators**~~

3.223 Where a PI provided payment services of the type described in paragraph 1(g) of

~~**In-flight applications**~~

~~**3.224** 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 payment institutions (PIs) and e-money institutions (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 under the Financial Services and Markets Act (2000) (FSMA) 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 (SUP).

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 European Union (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 Payment Services Regulations (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 (ASPSPs) and firms operating under exclusions from the scope of the PSRs 2017. 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 ser vices 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 Electronic Money Regulations 2011 (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, the PI or EMI 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 a 'reasonable period' 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. In relation to EMIs, this could include changes to the way that e-money is issued or to the range of payment services provided. 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 'a reasonable period'. In some circumstances, however, 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 Connect, 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 PIs and authorised and small EMIs. This is mostly due to authorised PIs and authorised 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 and small EMI also apply to an authorised PI and authorised EMI, some do not.

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

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

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

4.13 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;[~~17~~22]
- primary compliance contact;
- accounting reference date; and
- website and email address.

4.14 Pursuant to regulations 37(2) of the PSRs 2017 and 37(3) of the EMRs, as applicable, notifications must be made using Connect, or where a form is not provided, by written confirmation to our Customer Contact Centre.

Significant changes to the programme of operations

4.15 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**.

4.16 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.

[~~17~~22] 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.

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

Changes in methods of safeguarding

4.18 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.

4.19 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 – approval required by prospective controllers

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

4.21 In accordance with paragraph 4 of Schedule 3 to the EMRs and paragraph 5 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 a PI.[~~18~~23] Our approach to changes in control over EMIs and PIs will be the same as our approach to changes in control over firms authorised under FSMA (except where stated below). Chapter 11 of SUP (in particular, SUP 11.3 and SUP 11 Annex 6G) provides guidance on the change in control provisions of FSMA.

4.22 Section 178(1) of FSMA (as modified by Schedule 3 of the EMRs and Schedule 6 of the PSRs 2017, respectively) requires a person who decides to acquire or increase control over an EMI or PI to notify us in writing, and obtain our approval before proceeding with the change in control. This notice is referred to as a 'section 178' and can be found on our website. The notice can be submitted electronically to cic-notifications@fca.org.uk or sent by post. Section 191D(1) of FSMA (as modified) provides that a person who decides to reduce or cease to have control over an EMI or PI must give us written notice before making the disposition.

4.23 Where a person intends to acquire, increase or reduce control, or to cease to have control over a PI or an EMI, and this causes them to cross a control threshold (10%, 20%, 30% or 50%, or to acquire a holding that makes it possible to exercise a signif icant influence over the management of the authorised PI or EMI), that person must notify us before the proposed transaction.

4.24 Our approach 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 30 working days) to decide whether to approve, approve with conditions or object to the proposed changes in control.[~~19~~ 24]

[~~18~~23] 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.

~~19~~24 See section 178 to 191 of FSMA.

4.25 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 control to ensure the continued sound and prudent management of the EMI or PI.[2025] We must also consider the likely influence that the person will have on the EMI or PI but we cannot consider the economic needs of the market (see **Chapter 3 – Authorisation and registration**, especially regarding qualifying holdings).

4.26 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.

4.27 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 and PSRs 2017, when issuing a restriction notice we 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).

4.28 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. For example, a person who gives notice, and makes the acquisition to which the notice relates before the expiry date of the assessment period is guilty of an offence unless we have approved the acquisition or section 190A of FSMA applies. We may prosecute and if found guilty the person may be liable to an unlimited fine or given a prison sentence.

4.29 The form of notice that must be given by a person who decides to acquire or increase control over an EMI or 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 PI must contain the information and be accompanied by such documents as are required by the relevant FCA controllers form. A link to the forms is available on the e-money section of our website.

4.30 There is no form to notify us of a reduction or disposal of control in an EMI or PI. A notice should be giving in writing where this is going to occur. An email is acceptable (cic-notifications@fca.org.uk). This notification should include the name of an acquirer, and percentage of control to be disposed of.

Notifications from firms subject to changes in control

4.31 In relation to PIs and EMIs, we consider changes in control to be 'significant' in relation to changes in the circumstances of authorisation or registration. Therefore we expect to be notified where it becomes apparent to an institution that there will be a change in control, in good time before the change takes place. It is sufficient to provide a notification via email to cic-notifications@fca.org.uk, or send a letter to us. Under the PSRs 2017 there are no notification forms for institutions to complete. Notification forms are submitted by prospective controllers, as described above. PIs authorised or registered under PSRs 2017 will continue to submit the appropriate 'Application for

~~20~~25 Also see regulation 6(6)(a) of the EMRs.

a Change in Qualifying Holding' form, which is available on the payment institutions section of our website, until they are re-authorised or re-registered under PSD2.

Other changes affecting controllers and close links

4.32 A condition for authorisation and registration is that anyone with a qualifying holding in an authorised or small EMI or PI (a controller) must be a 'fit and proper' person. A further condition for authorisation or registration is that, if the applicant 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 or small 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 or regulation 37 of the EMRs. 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

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

4.34 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.

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

4.36 PIs and EMIs must also notify us of any changes in the details of existing PSD Individuals or 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 our website. EMIs should do this using the 'Amend an EMD Individual' form, which is available on our website.

4.37 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's or EMI's 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.

4.38 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.

4.39 Notification for PIs should be on the 'Notice to remove PSD Individual(s)' form which is available on 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

4.40 When 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 notify us using 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 authorisation

4.41 When a PI intends to change the payment services it is providing it needs to apply to us for approval. Both PIs and EMIs also need to apply to us for approval if they want to have a new requirement imposed or an existing requirement varied or removed.

4.42 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 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.

4.43 Applicants should complete and submit the 'Variation of PSD Authorisation/ Registration' or the 'Variation of EMD Authorisation/-Registration' form, as relevant. This is available on Connect and in some cases an application fee is required. This sets out the information that must be provided. We may, however, ask for more information if we consider it necessary to enable us to determine the application. If we consider that the proposed change will have an adverse effect on the EMI's or PI's fulfilment of the conditions for authorisation or registration, we have the power to vary the EMI's or PI's authorisation or registration by imposing such requirements as we consider appropriate.

4.44 No work will be done on processing the application until the full fee is received, where relevant. The fee is non-refundable.

4.45 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

4.46 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. We expect, however, 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

4.47 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

4.48 PIs and EMIs can request to cancel their authorisation or registration (regulations 10 and 14 of the PSRs 2017 and regulations 10 and 15 of the EMRs, respectively). They should use the 'Cancellation of Authorisation or Registration' form, which is available on Connect. We will remove the PI or EMI from the Financial Services Register once we have established that: there are no outstanding fees to either us or the Financial Ombudsman Service; 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 Register.

4.49 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 of the PSRs 2017 and regulation 37 of the EMRs (as applicable);
- 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

- the cancellation is desirable in order to protect the interests of consumers.

4.50 Where we propose to cancel an EMI's or PI's authorisation or registration other than at the EMI's 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**).

4.51 Our fee year runs from 1 April until 31 March, so if a PI or an 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

4.52 A change in legal status (e.g. 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 our website. EMIs should use the 'Change of Legal Status' form that is available on our website.

Part II: Notifications applicable only to authorised PIs and EMIs

4.53 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

4.54 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 EMIs 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) of the EMRs).

4.55 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 the payment services or e-money issuance (e.g. legal advice, training or security) or the purchase of standardised services, including market information services.

4.56 A proposed outsourcing arrangement, relating to both PIs and EMIs, that is classified as 'important' (pursuant to regulations 25(2) and (3) of the PSRs 2017 and regulations 26(2) and (3) of the EMRs as applicable) is more likely to be relevant to a PI or an EMI's compliance with the authorisation conditions than a proposed outsourcing arrangement 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.

4.57 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.

4.58 Registered Account Information Service Providers (RAISPs) will also need to ensure that any changes to their outsourcing arrangements do not cause them to stop meeting the conditions of registration. RAISPs may wish to notify us if they consider such changes to be important.

Auditors

4.59 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.

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

Part III: Notifications applicable only to small PIs and small EMIs

Change in regulatory status of a small PI

4.61 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, and a 'Cancellation of Authorisation or Registration' form in respect of its small PI registration.

4.62 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 regulatory status of a small EMI (regulation 16 of the EMRs)

4.63 If a small EMI no longer fulfils the conditions for registration outlined in regulation 8(2)(c) or (d) of the EMRs (as applied by regulation 15 of the EMRs)[~~21~~26] 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.

~~21~~

26 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 payment institutions (PIs), e-money institutions (EMIs) and registered account information service providers (RAISPs) to register their agents with us. It also covers the appointment of distributors by EMIs. Other chapters in this Approach 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 to 4.11 and 6.7 to 6.10, 6.14 to 6.18 and 6.24 to 6.47.

Introduction

PIs and EMIs

5.2 All PIs, EMIs and RAISPs 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, EMI or RAISP (i.e. a principal) in the provision of payment services (see the definition of agent in regulation 2 of the Payment Services Regulations 2017 (PSRs 2017) and regulation 2 of the Electronic Money Regulations 2011 (EMRs) as applicable).

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 confirm that PIs, EMIs and RAISPs are responsible for anything done or omitted by an agent. PIs, EMIs and RAISPs are responsible for their agents' acts or omissions to the same extent as if they had expressly permitted the act or omission. We expect PIs, EMIs and RAISPs to have appropriate systems and controls in place to oversee their agents' activities effectively.

5.4 An authorised PI, authorised EMI or RAISP wanting to use a passport to provide payment services into another European Economic Area (EEA) 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 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.

Registered account information service providers (RAISPs)

5.8 RAISPS are also subject to the requirements relating to agents in regulations 34 and 36(2) of the PSRs 2017. A RAISP wanting to use an agent to provide payment services in another EEA 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, EMIs and RAISPs who want to register an agent must do so through Connect. The same Connect form is used for agents of authorised and small PIs, EMIs and RAISPs.

5.10 The following information is 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 Directive (EU) 2015/849 (4AMLD) (or, in the United Kingdom, the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs))
- the identity of the directors and persons responsible for the management of the agent and, if the agent is not a payment service provider (PSP), and 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

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

AML internal control mechanisms

5.12 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.

5.13 We require a description of the internal control mechanisms that will be used to comply with the MLRs 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 applicable local legislation and regulation that implements 4AMLD and that such requirements are followed by their agents as required.

5.14 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.

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

Directors and persons responsible for the management of the agent

5.16 We must be provided with details of the director(s) and person(s) responsible for the management of the agent. For incorporated agents these are 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.

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

5.18 Where the agent is not itself a PSP (e.g. a PI, EMI or RAISP) we also need evidence that the relevant individuals are fit and proper persons. We ask PIs, EMIs and RAISPs to provide information about the individuals (including any adverse information) and certify that they have been assessed as fit and proper persons. PIs, EMIs and RAISPs should carry out their own fitness and propriety checks on their agents, on the basis of a 'due and diligent' enquiry before making the application. 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.

5.19 We expect PIs, EMIs and RAISPs 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:

- honesty, integrity and reputation
- competence and capability

5.20 For more information on the types of enquiries we expect PIs, EMIs and RAISPs 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.

5.21 We will use the enquiries made by the PI, EMI or RAISP to help our assessment of the fitness and propriety of the directors and persons responsible for the management of an agent.

Payment services for which agent is appointed

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

Unique identification code or number

5.23 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~~[22]~~[27] (LEI) this must also be provided. For EEA agents an LEI or another identification number should be provided, as specified in Annex 1 of the European Banking Authority's (EBA) Regulatory Technical Standards on the framework for cooperation and exchange of information between competent authorities for passport notifications under PSD2.~~[23]~~[28] Also see **Chapter 6 – Passporting** on passporting activities.

Additional information and changes to information supplied

5.24 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.

5.25 Once an application has been submitted, before it has been determined and on an ongoing basis, applicants must without undue delay 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.

Decision making

5.26 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.

5.27 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.

5.28 An application to appoint an agent may be combined with an application for authorisation or registration – in which case it will be determined in accordance with the timetable for that application.

Approval

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

5.30 Under regulation 34(14) of the PSRs 2017 and regulation 34(12A) of the EMRs, PIs, EMIs and RAISPs must notify us of the date when they start to provide payment services in another EEA State through a registered EEA agent. PIs, EMIs and RAISPs should notify

---

~~22~~27 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.

~~23~~28 These draft 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~~-psd2. These RTS will take effect as a Commission Delegated

Regulation once published in the EU's Official Journal. We will update this Approach Document as necessary after the RTS come into force.

us using Connect. We must notify such date to the relevant host state competent authority.

Refusal

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

a. 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

b. we are not satisfied that the directors and persons responsible for the management of the agent are fit and proper persons

c. 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 MLRs in the UK) is taking place, has taken place or has been attempted
- the provision of services through the agent could increase the risk of money laundering or terrorist financing

5.32 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.

5.33 **Chapter 14 – Enforcement** provides more information on what we will do if we propose to refuse to include an agent on the Financial Services Register.

Cancellation of agents

5.34 To cancel an agent registration the principal must submit a *Remove PSD agent* or *Remove EMD agent* application through Connect. We will update the Financial Services Register to show that the agent is no longer registered to act for the principal once we have finished processing the notification.

5.35 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 Connect (see **Chapter 6 – Passporting**). Please note that if a PI, EMI or RAISP removes its last EEA agent within one EEA State and does not have a branch in that State, the relevant PSD2 or 2EMD establishment passport must be cancelled.

Changes to agent details

5.36 The principal must submit an *Amend PSD agent* or *Amend EMD agent* application

through Connect to amend the details of an agent.

5.37 We will assess the impact of the change against the agent registration requirements. If the change is approved we will update the Financial Services Register as soon as possible. If we need more information we will contact the PSP, and if the change is not approved we will follow the refusal process set out above.

Notifying HMRC

5.38 The PI or EMI should make sure that Her Majesty's Revenue and Customs' (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 payment institutions (PIs), authorised e-money institutions (EMIs) and registered account information service providers (RAISPs) will need to go through if they wish to provide payment services or, in the case of authorised EMIs, to issue, distribute or redeem e-money in another European Economic Area (EEA) State. It also tells PIs and EMIs authorised in another EEA State and RAISPs registered in another EEA State how we will deal with notifications to provide payment services or, in the case of authorised EMIs, to issue, distribute or redeem e-money in the UK that we receive from their home state competent authority.

~~**6.2** The European Banking Authority (EBA) has published draft Regulatory Technical Standards (RTS) specifying the method, means and details of the cross-border cooperation between competent authorities in the context of passporting notifications of payment institutions (Passporting RTS).[24] Once published in the European Union's Official Journal, the Passporting RTS will take effect as a Commission Delegated Regulation. We will update this Approach Document in line with the Passporting RTS after they take effect. Presently, this chapter should be read alongside the draft final version of the Passporting RTS.~~

6.2 This chapter should be read alongside the Commission Delegated Regulation 2017/2055 with regard to regulatory technical standards for the cooperation and exchange of information between competent authorities relating to the exercise of the right of establishment and the freedom to provide services of payment institutions (Passporting RTS).[29]

6.3 Directive (EU) 2015/2366 (PSD2) introduces two new payment services that can be passported within the EEA: payment initiation services (PIS) and account information services (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 Registered Account Information Service Provider (RAISP).

Introduction

6.4 Passporting is the exercise by a business of its right to carry on activities and services regulated under EU legislation in another EEA State on the basis of authorisation or registration in its home EEA State. The activities may be carried on through an establishment in the host state (an 'establishment' passport) or on a cross-border services basis without using an establishment in the host state (a 'service' passport). A physical presence established in another EEA State by a UK authorised PI, RAISP or UK authorised EMI is referred to as an 'EEA branch' (see Q45 in PERG 15.6 for further guidance on the criteria for determining whether a firm has an establishment in another EEA State). Regulations 26 to 30 of the Payment Services Regulations 2017 (PSRs 2017) and regulations 28 to 30 of the Electronic Money Regulations 2011 (EMRs) set out the respective procedures for the exercise of passporting rights by authorised PIs, RAISPs and authorised EMIs.

6.5 Passporting rights are only available to authorised PIs, RAISPs and authorised EMIs

(except authorised EMIs whose head office is situated outside the EEA), not small PIs or small EMIs.

24 The draft final version of the Passporting RTS is available here:

29 The Commission Delegated Regulation 2017/2055 is available here: https://www.eba.europa.eu/-/eba-publishes-final-draft-technical-https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CEL-standards-on-cooperation-and-exchange-of-information-for-passporting-under-psd2 EX:32017R2055&from=EN-

Authorised PIs

6.6 Passporting rights extend to all payment services which the authorised PI is authorised to carry on but does not, in our view, extend to other activities that authorised PIs may carry on that are ancillary to the provision of payment services (see regulation 32 of the PSRs 2017). Whether an authorised PI may carry on those other activities in another EEA State will depend upon local law; businesses may therefore wish to take professional advice if they think that they are likely to be affected by this.

6.7 A UK authorised PI may provide services in another EEA State through an agent (an 'EEA Agent'). Such an agent may be based in the UK (in which case the PI will require a services passport) or in another EEA State (in which case the PI will likely require an establishment passport). Agents must be registered (see **Chapter 5 – Appointment of Agents and Distributors**) and details provided as part of the passport application.

RAISPs

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 to 30. As such, RAISPs are permitted to exercise their right to passport in respect of AIS (PSD activity 8, Annex 1 of PSD2). RAISPs may also provide services in another EEA State through an agent. ~~The RAISP must provide details~~, and the same conditions apply as for agents of ~~agent(s) as part of its passporting application~~authorised PIs.

Authorised EMIs

6.9 A UK authorised EMI may carry on payment services in another EEA State, including through an EEA agent (the same passport conditions apply as for PSD agents). A UK ~~authorised~~ authorised EMI may also issue, redeem or distribute e-money in another EEA state and it may 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 ~~notif~~application procedures (i.e. those applicable to a service or establishment passport as appropriate) and provide us with a list of all distributors, including their name, address and (in the case of natural persons) date and place of birth, together with any other information requested. We will then communicate this information to the host state competent authority.

Further guidance

6.11 PERG 15.6 provides further guidance on when we consider a passport notification needs to be made by an authorised PI or a RAISP. The passporting section of our website includes answers to frequently asked questions with regard to authorised PIs, RAISPs and authorised EMIs.

Making a passport application

6.12 The procedure for making an application to exercise passport rights depends upon the precise way in which the applicant wishes to carry on payment services in another EEA State. The procedures for all types of passport application are set out below.

Application ('Notice of intention')

6.13 Where an applicant intends to provide payment services or, in the case of an authorised EMI, to issue, distribute or redeem e-money, in another EEA State for the first time, either on a freedom of services or establishment basis, regulation 27 of the

PSRs 2017 and regulation 28 of the EMRs (as applicable) require the applicant to submit to us a notice of intention to passport. Applicants must submit this notice of intention through Connect.

6.14 Our notice of intention forms are designed to ensure that we have the information that the Passporting RTS require us to pass to the host state competent authority. Our passporting forms are:

- Notice of intention to exercise the freedom to provide services, with or without agent or distributor
- Notice of intention to exercise right of establishment, either through a branch, or with an agent or a distributor

6.15 The notice of intention for all passport applications must include:

- the applicant's name, head office address, authorisation or registration number, Companies House number, and Legal Entity Identifier (LEI) (where it has one)
- the name, email address and telephone number of the contact person within the applicant
- the EEA State(s) where a branch or agents are to be established or services are to be provided (the host state)
- the payment services and/or e-money services that the applicant intends to carry on in the host state
- details of any outsourcing of operational functions in the host state

6.16 An LEI is a unique globally-recognised code, issued under these arrangements: https://www.leiroc.org. We appreciate that few applicants will have an LEI, so it will only need to be provided where available.

6.17 We are required to assess the completeness and accuracy of the information provided in all passporting applications that we receive in line with Passporting RTS Article 4. Where we deem this information to be incomplete or inaccurate, we will inform the applicant without delay, indicating in which respect we consider the information to be incomplete or inaccurate.

Notification process

6.18 Once we have received a complete application, we will check that the services that the applicant intends to carry on 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 and regulation 28(3) of the EMRs, 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-

applicants to ensure that the information provided is as complete and accurate as possible on first submission to avoid delays in the passporting approval process. We will inform the applicant when 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 The host state competent authority will then have a month from its receipt of the information in which to make an assessment 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 paragraph 6.40 for more details on the assessment of information received from host state competent authorities).

6.22 If we are minded to reject an application, we must give a warning notice to the applicant, the responses to which we will consider in making our final decision.

6.23 We must provide our decision within three months of receipt of the notification from the applicant (again dated from receipt of complete information). The decision to grant or reject the application (including the decision whether or not to register a branch) will be communicated to both the applicant and the host state competent authority.

6.24 In addition to the power to refuse an application, we can cancel existing registrations of branches (regulation 28(2)(a)(i) of the PSRs 2017 and regulation 29(1) of the EMRs) and EEA agents (regulation 35(1) of the PSRs 2017 and regulation 35(1) of the EMRs). We also have powers under regulation 7 of the PSRs 2017 and regulation 7 of the 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 applicant, we will follow a decision making process equivalent to that described in Part III, **Chapter 3 – Authorisation and registration**.

6.25 An applicant may not commence passporting until it has received notice of our decision permitting it to passport. EEA agents and branches are also only permitted to commence their activities in a host state once they are entered on the Financial Services Register. Therefore applicants must not undertake any activity – whether 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 the agent(s) or branch appears on the Financial Services 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 the date on which we receive complete and accurate information from them.

6.26 Authorised PIs, and authorised EMIs and RAISPs are required to notify us of the date on which they commence their activities in another EEA State (through a branch, agent or distributor). The start of activity notification must be submitted via Connect. We will then inform the host state competent authority accordingly.

Service passports – not involving an EEA agent or distributor

6.27 In addition to the general information required in all passport applications (see paragraph 6.~~12~~15), notice of an applicant's intention to exercise its freedom to provide services without the use of agents or distributors must also include the intended start date from which payment or e-money services will be provided~~.~~ in line with Passporting RTS Article 14(1)(g).

Establishment passports involving a branch

6.28 In addition to the general information required in all passport applications (see paragraph 6.~~12~~15), notice of an applicant's intention to exercise its right of establishment that involves the use of an EEA branch must also include, in accordance with Passporting RTS Article 6, details such as:

- the address of the proposed branch
- the name, email and telephone number of the people responsible for managing the proposed branch
- a description of the organisational structure of the proposed branch
- a business plan demonstrating that the proposed branch will be able to employ appropriate and proportionate systems, resources and procedures to operate soundly in the host state
- a description of the governance arrangements and internal control mechanisms of the proposed branch

Services or establishment passports involving use of EEA agents or distributors

6.29 The provision of payment services in other EEA States through the use of agents may require either an establishment or services passport, depending on the circumstances. The same applies to authorised 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 we consider that the use of the agent/distributor comes under a services passport rather than an establishment passport, we will be obligated to state the reasons for this decision in the notification to the host state competent authority. In making this assessment, we will take into account the guidance provided by the Commission Interpretative Communication (Freedom to provide services and the interest of the general good in the Second Banking Directive (97C 209/04)).

6.31 The application processes for passports using EEA agents and distributors are very similar. As with applications for branch and services passports, applicants will be required to provide the general information set out in paragraph 6.~~12~~15. In both cases, applicants will also be required to provide the following additional information in line with Passporting RTS Article 10:

- a description of the internal control mechanisms that will be used to comply with the obligations in relation to money laundering and terrorist financing
- if the agent or distributor is a natural person, the individual's:
  - name, date and place of birth
  - unique identification number (a list of the information required as a unique identification number for each country can be found in Annex I of the Passporting RTS.

  - registered business address, telephone number and email
- if the agent or distributor is a legal entity, the entity's:
  - unique identification number or LEI (where available)

- telephone number and email
- name, date and place of birth of its legal representatives

6.32 Applicants wishing to use EEA agents must also provide the information required by regulation 34(3)(a) of the PSRs 2017 and regulation 34(3)(a) of the EMRs as applicable (use of agents). This covers the identity and contact details of directors and persons responsible for the management of the agent to be used. For agents other than PSPs (i.e. those without authorisation in their own right) it covers evidence that the directors and management are fit and proper persons (please see paragraphs 6.~~35~~34 to 6.37.

6.33 Where firms are operating through agents on an 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. their name, address, telephone number and email.~~25~~30

Fitness and propriety

6.34 Where an applicant seeks to establish a branch, we will assess the fitness and propriety of the management of the proposed branch in the same way as we assess that of other PSD Individuals or EMD Individuals – see **Chapter 3 – Authorisation and registration**.

6.35 The registration of an EEA agent depends on the directors and persons responsible for the management of the agent being fit and proper. As per **Chapter 5 – Appointment of Agents**, the authorised PI, RAISP or authorised EMI should carry out its own fitness and propriety review of its proposed agents before completing the application form to register an EEA agent. We will use the enquiries made on these persons to help in our assessment of these matters. Under regulation 34(3)(a)(iii) of the PSRs 2017, regulation 34(3)(a) of the EMRs, the applicant has to provide us with evidence the directors and persons responsible for the management of the agent are fit and proper persons. We may also require the applicant to provide us with such further information as we reasonably consider necessary to enable us to determine the application. The information on the fitness and propriety of directors and managers of agents will be included in the notification that we must make to the host state competent authority.

6.36 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."

6.37 We must take account of any relevant information provided by the host state competent authority, but we are entitled to disagree with any assessment that they make. If we disagree, we will be required to explain our reasons for doing so. If our assessment of the information provided is unfavourable to the applicant, we will refuse ~~to register the EEA agent or branch and, where appropriate, refuse the passporting application (see paragraph 6.22).~~

~~25~~30 At the time of issuing this Approach Document, the EBA has published draft Regulatory Technical Standards on central contact points under PSD2. ~~The EU is consulting on these proposed standards (EBA-CP-2017-09).~~ We will update this document as required in line with the final standards after they are published in the EU's Official Journal.

to register the EEA agent or branch and, where appropriate, refuse the passporting application (see paragraph 6.22).

Making changes

6.38 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 notif ication and may include:

- changes to the name or address of the firm or agent engaged in another EEA State
- adding or removing an agent or distributor
- adding or 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
- changes to the organisational structure or governance arrangements of the branch or agent

6.39 A notification of changes will be subject to a similar review process as a new passport notification. For example, if an EEA agent is being added to an existing passport, the process will be the same as the one described above and it may take up to three months before the agent may become active. Please note that firms are required to submit start of activity notifications for each new agent added to existing passports.

Incoming EEA authorised PIs, RAISPs and authorised EMIs

6.40 Firms that are authorised or registered in another EEA State that wish to provide payment services or issue, distribute or redeem e-money in the UK should refer to their home state competent authority for instructions on making a passport application. These EEA authorised EMIs, EEA authorised PIs and EEA RAISPs will appear on the register of their home state and the EBA register, but not our Financial Services Register.

6.41 When we receive a passport notification from the applicant's home state competent authority, we are required to assess the information and provide relevant information to the home state competent authority, especially relating to reasonable grounds for concern with regard to money laundering and terrorist financing involvement. Where we have concerns, we must 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.

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

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

6.44 If an EEA authorised PI, EEA RAISP 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 (e.g. to provide investment services under the Markets in Financial Instruments Directive (MiFID)).

Supervision of incoming EEA PIs and EMIs

6.45 We are responsible for supervising compliance by a UK authorised PI, UK authorised EMI or UK RAISP with its capital requirements and the conditions of authorisation or registration, regardless of where in the EEA it carries on payment services. We are not, however, responsible for supervising compliance with capital requirements or conditions of authorisation or registration by an EEA authorised PI, EEA authorised or EEA RAISP.

6.46 We are responsible for supervising compliance with the conduct of business requirements of the PSRs 2017 and EMRs in relation to payment services and e-money services being carried on from an establishment in the UK (e.g. 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 (e.g. under a services passport).

6.47 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 the 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. For further information see paragraph 6.33.

6.48 We will exchange information about authorised PIs, authorised EMIs, EEA authorised PIs and EEA authorised EMIs with other competent authorities in accordance with the:

- PSRs 2017 and EMRs (as applicable)
- Passporting RTS
- 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~~[26] authorities[31]

6.49 In particular, we are obligated to provide relevant competent authorities with all relevant or essential information relating to the exercise of passporting rights by an authorised PI, RAISP or authorised EMI, including information on breaches or suspected breaches of the PSRs 2017, EMRs or applicable money laundering and terrorist financing laws.

~~26~~31 At the time of issuing this Approach Document, the EBA has ~~not~~ published ~~these~~draft RTS on home-host cooperation under PSD2. We will update this Approach Document as necessary after any such RTS come into force after they are published in the EU's Official Journal.

7 Status disclosure and use of the FCA logo

7.1 This chapter explains what payment institutions (PIs) and e-money institutions (EMIs) may say about their regulatory status and the restriction on the use of our 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 registered account information service provider (RAISP) from making a factual statement about its regulatory status (as is required in the information requirements in Part 6 of the Payment Services Regulations 2017). **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 Payment Services Regulations 2017 (PSRs 2017) conduct requirements apply to all payment service providers (PSPs) — including e-money institutions (EMIs) when providing payment services. This excludes credit unions, municipal banks and the National Savings Bank. The Electronic Money Regulations 2011 (EMRs) 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
- micro-enterprise (see Glossary of Terms for definition)
- 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. There are, however, exceptions to this.

8.10 Where one of the PSPs is located outside the European Economic Area (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 the Financial Services and Markets Act 2000 (FSMA) (e.g. 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 The Consumer Credit Sourcebook (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 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 regulation 32(2) of the EMRs. These 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. There are, however, some exceptions to this and the PSP needs to be aware of how the two regimes interact. We set out more detail in paragraphs 8.64 – 8.68.

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 the 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 relating to communications and financial promotions and BCOBS 6 relating to cancellation). It also sets out which provisions of BCOBS do not apply to payment services where Parts 6 and 7 of the PSRs 2017 apply (e.g. 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 (e.g. some savings accounts) the requirements in Parts 6 and 7 of the PSRs 2017 do not generally apply to conduct that relates to the account taken as a whole, and so the PSP will need to comply with the requirements in BCOBS. 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. Provisions in the PSRs 2017 that apply to payment transactions will, however, apply to individual payment transactions within the scope of the PSRs 2017 that are made to and from accounts which are not payment accounts. This means, for example, that the PSRs 2017 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. Provisions in the PSRs 2017 that apply only to payment accounts (e.g. regulation 89(1)) will not apply to non-payment accounts and the relevant provisions in BCOBS will apply instead. Guidance on the meaning of payment account is set out in PERG 15.

8.23 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).

8.24 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

Distance Marketing Directive

8.25 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.

8.26 The rules implementing the DMD in relation to retail banking services can be found in the Handbook 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 the Handbook in CONC.

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

8.27 Regulation 924/2009 is a directly applicable European Union (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. We are the competent authority and the Financial Ombudsman Service is the out-of-court redress provider for this regulation.

8.28 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 we are the UK competent authority.

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

8.29 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.

8.30 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 the Handbook in CONC 2.8.

8.31 For other payment services and the 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)

8.32 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).

8.33 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)

8.34 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.

8.35 In providing customers with details of their service, PSPs and e-money issuers must avoid giving customers misleading impressions or marketing in a misleading way, e.g.:

- 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 otherwise implying that such a provider is a bank
- advertising interbank exchange rates that will not be available to the majority of customers

8.36 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 We are 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 will not be classed as "payment accounts" under the PARs (e.g. 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). PSPs could, however, 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. This is, however, 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 our 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) of NIS. 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[27]~~ regulation[32], 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 which relate to user information. Any requirements in the PSRs 2017 relating to user information are distinct from requirements under data protection law. PSPs will need to put appropriate procedures in place to ensure that they comply with their obligations under the PSRs 2017 and their obligations under data protection legislation cumulatively.

8.54 There are various requirements in the PSRs 2017 for PSPs to have or obtain the user's "consent" or "explicit consent" in relation to the provision of payment services (e.g. consent to a payment transaction). "Consent" and "explicit consent" must be interpreted in the context they are used, and in line with the purpose and scope of PSD2. Where "consent" or "explicit consent" is required under the PSRs 2017, we include guidance in this chapter regarding the nature of such consent.

8.55 "Consent" and "explicit consent" are also concepts under data protection law, where they are interpreted in a specific way. For more detail regarding the way explicit consent is interpreted under data protection law, PSPs should have regard to the Information Commissioner's Office guidance on "explicit consent". The interpretation of "consent" and "explicit consent" under data protection law should not be read across into the requirements under the PSRs 2017.

~~27~~32 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

8.56 Similarly, "sensitive payment data" is referred to in the PSRs 2017 and this is a different concept to "sensitive personal data" under data protection law.

Anti-money laundering and terrorist financing legislation

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

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

8.59 For businesses supervised by us under the MLRs, the Joint Money Laundering Steering Group has provided guidance on interpreting these obligations and we have a financial crime guide. For businesses supervised by HMRC under the MLRs (e.g. those only undertaking the payment service of money transmission) HMRC has provided guidanceoncomplyingwithAMLandCFTobligations.

8.60 **Chapter 19 – Financial Crime** contains further details about these requirements.

Part I: Information requirements

8.61 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 ongoing 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 contract that does not include the particular payment service involved.

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

8.63 The corporate opt out applies to all of the information requirements under Part 6 of the PSRs 2017 (see under "General" at the start of Part II of this chapter).

8.64 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. There are, however, 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.

8.65 Regulation 41(2) provides that:

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

8.66 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 (e.g. under CONC or the CRA).

	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	Regulation 51 will **not** apply to the overdraft.	Regulation 51 will **not** apply. Termination will be governed by applicable provisions in the CCA.

8.67 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.

8.68 The requirements of the PSRs 2017 and the consumer credit regime apply cumulatively, however, 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 (Standard European Consumer Credit Information) for a credit card would not need to be duplicated to meet requirements under regulation 48 of the PSRs 2017. However, any information **not** included in the SECCI or other pre-contractual documentation would still need to be provided to the customer in accordance with regulation 48 of the PSRs 2017.

Communication of information (regulation 55)

8.69 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.

8.70 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.

8.71 In contrast, a requirement to make information available means that the customer can be required to take active steps to obtain the information (e.g. 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). However, access must be possible and the information must be readily available.

8.72 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. If, however, they send an email to the email address provided by the customer 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.

8.73 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.

8.74 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 of PSD2, 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. We acknowledge, however, that many forms of media are capable of meeting the criteria of being a durable medium.[~~28~~33]

8.75 The definition of durable medium has been considered recently by the CJEU in the context of internet sites. It was the CJEU's finding that, for an e-banking portal or other website itself to be a durable medium, it must:

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

28~~33~~ https://www.fca.org.uk/firms/durable-medium, also see CP17/7 Insurance Distribution Directive implementation – consultation paper I

8.76 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, or if the website is not available after the customer closes their account.

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

8.78 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).

8.79 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)

8.80 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 provide the information beforehand), the PSP must provide the customer the information in the table below.

8.81 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 (e.g. the provider's Financial Services Register number).
Details of the payment service(s) to be provided	

~~**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 (e.g. 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 regulation 100 (authentication) of the PSRs 2017 although, in our view, this does not require PSPs to set out details of their technical solutions relating to authentication in the framework contract.~~

~~Details of when a payment order will be deemed to have been received in accordance with regulation 81 of the PSRs 2017 (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 of the PSRs 2017.~~

	Where applicable, the fact that a spending limit may be agreed for a payment instrument attached to the account (e.g. a maximum daily withdrawal limit on an ATM card), although the spending limit itself (e.g. £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 (i.e. where a payment is initiated through a payment initiation service provider (PISP), details of the amounts charged by that PISP do not need to be provided by the account servicing payment service provider (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 of the PSRs 2017, this must be specified here. If the PSP will make a charge for providing or making information available in accordance with regulation 56(2) of the PSRs 2017 (e.g. 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 (e.g. 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) of the PSRs 2017). This information requirement will not be relevant where a payment service is provided in relation to payment transactions that consist of the placing, transferring or withdrawal of funds covered by a credit line provided under a regulated agreement for the purposes of Chapter 14A of Part 2 of the Regulated Activities Order (as regulations 50 and 51 do not apply in such circumstances). Where reference interest rates are being used, agreement, of how, and with what frequency changes in actual interest 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 (e.g. 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	Where relevant, 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. Where relevant, 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 (e.g. 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 EU legal obligations of the PSP. This information requirement will not be relevant where section 98(A)(4) of the Consumer Credit Act 1974 applies (i.e. it will not apply to CCA regulated credit cards).

	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 (e.g. that the PSP will be liable for unauthorised or incorrectly initiated or executed payment transactions, as long as, where applicable, the claim is made within the time limits specified above) under regulation 76 of the PSRs 2017 or, as the case may be, section 83 of the Consumer Credit Act 1974, and regulations 91 and 92 of the PSRs 2017. 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 (e.g. a direct debit or card transaction).
Information about the length of the contract, variation of terms and termination	The duration of the contract and, where relevant, customer and PSP termination rights, and the terms under which the PSP can unilaterally vary the contract. The information requirements relating to variation and termination will not be relevant where a payment service is provided in relation to payment transactions that consist of the placing, transferring or withdrawal of funds covered by a credit line provided under a regulated agreement (as regulations 50 and 51 of the PSRs 2017 do not apply in such circumstances).
Information on applicable law and disputes	Details of the law applicable to the contract, the competent courts, the availability of the Financial Ombudsman Service or (for users that would not be eligible to complain to Financial Ombudsman Service) another dispute resolution service if the PSP uses such a service, any other alternative dispute resolution procedures available to the customer (e.g. under the Online Dispute Resolution Regulation (EU 524/2013), how to access them (see **Chapter 11 - Complaints handling**) and the possibility to submit complaints to us.

Information during period of contract (regulation 49)

8.82 The customer is entitled to request the information specified in Schedule 4 of the PSRs 2017 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)

8.83 Where a payment service is provided in relation to payment transactions that consist of the placing, transferring or withdrawal of funds covered by a credit line provided under a regulated agreement, regulation 50 of the PSRs 2017 does not apply. See paragraph 8.64 for further details.

8.84 For most changes to the framework contract, or to the information that has to be disclosed before the framework contract is entered into (i.e. the information detailed in paragraph 8.80), 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.

8.85 Some account terms and conditions will contain provisions relating to other services which are not "payment services" as defined by the PSRs 2017. In such cases the obligation to notify changes under regulation 50 of the PSRs 2017 does not extend to non-payment services that are outside the scope of the pre-contract disclosure requirement. For banks and building societies, however, the BCOBS requirements on appropriate information and making changes may apply to such services.

8.86 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 without charge at any time before that date

8.87 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.

8.88 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.

8.89 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 either:

- 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); or

- the changes are more favourable to the customer

8.90 The PSP must inform the customer of any change to the interest rate 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.

8.91 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; e.g. 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.

8.92 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) of the PSRs 2017 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 in paragraph 8.81.

8.93 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. The notification requirement does not, however, 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.

8.94 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. It is recognised, however, 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)

8.95 Where a payment service is provided in relation to payment transactions that consist of the placing, transferring or withdrawal of funds covered by a credit line provided under a regulated agreement, regulation 51 of the PSRs 2017 does not apply. See paragraph 8.64 for further details.

8.96 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 six months or more, no charge may be made for termination. Regular ser vice 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.

8.97 If agreed in the framework contract (and subject to the UTCCRs or 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.

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

Transaction information under a framework contract

Before execution (regulation 52)

8.99 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)

8.100 Under regulations 53 and 54 of the PSRs 2017 the PSP must provide its customer with certain information on transactions.

8.101 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 8.70, as the information needs to be provided, it must be sent or given to the customer. We have set out in paragraph 8.74 some details relating to the meaning of durable medium.

8.102 Where a PSP's customer is the payer, the framework contract may include a condition that the customer may require the information to instead be provided or made available at least once a month, free of charge and in an agreed manner which enables the payer to store and reproduce the information unchanged.

8.103 It is our view that this means that the contract may provide for the customer to choose to receive information in an alternative manner, but that the customer cannot exercise this option simply by agreeing to the terms and conditions. A separate agreement to the alternative provision of the information will need to be actively made by the customer. Without this, the PSP will need to provide the information at least once a month on paper or another durable medium.

8.104 Where a PSP's customer is the payee, a PSP may provide in its framework contract that the information will instead be provided or made available at least once a month, free of charge and in an agreed manner which enables the payer to store and reproduce the information unchanged.

8.105 In both cases 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. Our view is that documents uploaded to a bank's e-banking portal may meet this requirement if they may easily be downloaded or printed, and it is explained clearly to customers why they should do so. We would, for example, expect PSPs to make customers aware of how long the information will remain available. The portal should not give the impression that it provides independent permanent storage if this is not, in fact, the case.

8.106 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).

8.107 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 in which the payer's payment account is debited or in the currency used for 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

8.108 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 Regulation requires, 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)

8.109 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

8.110 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 (e.g. by telephone) where it is not practicable to do so) and information required before individual payment transactions.

8.111 The PSP must provide information on the main characteristics of the payment service. 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 of the PSRs 2017 that must normally be disclosed prior to being bound by a framework contract (as specified in Schedule 4 (e.g. the website URL))

8.112 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.

8.113 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. The PSP must, however, enable the customer to check the amount of funds stored.

8.114 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 (i.e. they can agree that there is no need to communicate the changes on paper or another durable medium).

8.115 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)

8.116 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 (e.g. by telephone) where it is not practicable to do so beforehand), 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 of the PSRs 2017
- 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)

8.117 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. We consider, however, 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)). Where the service is payment initiation 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. This 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 Financial Ombudsman Service, notification of the availability of the Financial Ombudsman Service (or, for users that would not be eligible to complain to the Financial Ombudsman Service, another dispute resolution service if the PSP uses such services), any other alternative dispute resolution procedures available to the customer (e.g. under the Online Dispute Resolution Regulation (EU 524/2013)) and how to access them (Schedule 4, paragraph (7)(b)). See paragraphs 11.9 to 11.15 on providing information about complaints procedures.

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

8.119 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.

8.120 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)

8.121 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.

8.122 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

8.123 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 provided by the PISP to the payer and payee under regulation 44(1)(b) of the PSRs 2017. The ASPSP is not obligated to provide or make available this reference to the customer.

After the receipt of the payment order (regulation 45)

8.124 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 (regulation 81 of the PSRs 2017 sets out when payment orders for future dated payments are deemed to be received):

- a reference to enable the payer to identify the transaction (and if appropriate the information relating to the payee, e.g. 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)

8.125 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 (e.g. name of the payer and invoice number). The Funds Transfer Regulation requires, 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)

8.126 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)

8.127 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)

8.128 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 (i.e. "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 of the PSRs 2017.

Information on additional charges or reductions (regulation 58)

8.129 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 (e.g. an additional charge for using a credit card) this information must be advised to the customer before the start of the payment transaction.

8.130 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 of the PSRs 2017 and may also be in breach of the Consumer Protection from Unfair Trading Regulations.

8.131 The customer is not obligated 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 of the PSRs 2017.

8.132 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).

Burden of proof (regulation 59)

8.133 The burden of proof is on the PSP to show that it has met the information requirements in Part 6 of the PSRs 2017. 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)

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

8.135 RAISPs must always provide details of all charges payable by the customer to the RAISP and, where applicable, a breakdown of those charges.

8.136 RAISPs must also provide any information specified in Schedule 4 of the PSRs 2017 which is relevant to the service provided. What is 'relevant' will depend on the nature of the service and the circumstances. We consider, however, 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 RAISP accesses the customer's account with the ASPSP. This should be presented in a way which is easy for customers to understand
- for customers who are eligible to take complaints to the Financial Ombudsman Service, notification of the availability of the Financial Ombudsman Service (or, for users that would not be eligible to complain to the Financial Ombudsman Service, another dispute resolution service if the PSP uses such services), any other alternative dispute resolution procedures available to the customer (e.g. under the Online Dispute Resolution Regulations (EU 524/2013)) and how to access them). See paragraphs 11.9 to 11.15 on providing information about complaints procedures.
- any contractual clause on the law applicable to the framework contract and the competent courts

8.137 The burden of proof is on the RAISP to show that it has met the relevant information requirements.

8.138 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

8.139 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)

8.140 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.

8.141 Part 7 of the PSRs 2017 also applies where a payment service is provided in relation to payment transactions that consist of the placing, transferring or withdrawal of funds covered by a credit line provided under a regulated agreement, although certain provisions are disapplied.

8.142 Regulation 64 of the PSRs 2017 sets 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 76(1)-(4) and 77(1)-(5) (rectification of liability for unauthorised transactions) do not apply
- regulation 74 as it applies in relation to regulation 76 (PSP's liability for unauthorised payment transactions) does not apply. This means that the notification requirements under regulation 74 do not apply in respect of unauthorised transactions, but do apply to incorrectly executed transactions in these circumstances
- regulation 76(5) and 77(6) applies as if—
  - in regulation 76(5), the reference to an unauthorised payment transaction were to a payment transaction initiated by use of a credit facility in the circumstances described in section 83(1) of the Consumer Credit Act 1974 (liability for misuse of credit facilities);

– the references to complying with regulation 76(1) were to compensating the payer for loss arising as described in section 83(1) of the Consumer Credit Act 1974.

8.143 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 (e.g. 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	Regulation 71(2)-(5) of the PSRs 2017 applies to overdrafts. This is because Regulation 71(2) - (5) is only disapplied where s98A(4) of the CCA applies. Section 98A(4) of the CCA does not apply to overdrafts.	Regulation 71(2)-(5) does not apply to credit cards. Section 98A(4) of the CCA applies.
(2) Regulations 76(1)-(4) and 77(1)-(5) - rectification of and liability for unauthorised transactions - and regulation 74 (as it applies to regulation 76)	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 transactions occur when the customer is in a debit position, regulations 76(1)-(4) and 77(1)-(5) will not apply and the notification requirements under regulation 74 will also not apply in respect of unauthorised transactions. 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 76(1) - (4) and 77(1) - (5) will not apply and the equivalent regime in the CCA will apply. The notification requirements in regulation 74 will also not apply in respect of unauthorised transactions.

	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?**	
(3) regulations 76(5) and 77(6) - rectification of and liability for unauthorised transactions	Yes, they apply as if (i) in regulation 76(5), the reference to an unauthorised payment transaction were to a payment transaction initiated by use of a credit facility in the circumstances described in section 83(1) of the Consumer Credit Act 1974 (liability for misuse of credit facilities) and (ii) the references to complying with regulation 76(1) were to compensating the payer for loss arising as described in section 83(1) of the Consumer Credit Act 1974	Yes, they apply as if (i) in regulation 76(5), the reference to an unauthorised payment transaction were to a payment transaction initiated by use of a credit facility in the circumstances described in section 83(1) of the Consumer Credit Act 1974 (liability for misuse of credit facilities) and (ii) the references to complying with regulation 76(1) were to compensating the payer for loss arising as described in section 83(1) of the Consumer Credit Act 1974

Requirements for RAISPs (regulation 63(4))

8.144 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) (payment service user's obligation to keep personalised security credentials safe)
- regulation 98 (risk management)
- 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)

8.145 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).

8.146 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.

8.147 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 their own and the payer's PSPs' charges (known in SWIFT terms as 'BEN') are not permitted.

8.148 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))

8.149 The payee's PSP may not prevent the payee from requesting payment of a charge by the payer for, 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).

8.150 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)

8.151 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 (e.g. 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. The procedure for giving consent to execute a payment transaction could be in writing, by using a payment card and PIN number, through a website, by telephone or by use of a password. For consent to be valid it must be clear, specific and informed. Regulation 100 of the PSRs 2017 sets requirements regarding the application of strong customer authentication in certain circumstances. **Chapter 20 – Authentication** provides further information.

8.152 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 (e.g. whether it is an instruction for a future dated payment or an immediate

customer. This will depend on the particular circumstances of the payment transaction in question (e.g. 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,

8.153 If consent has been given to a series of payment transactions (e.g. 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) of the PSRs apply to any payment transaction due within that time period.

8.154 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 is 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.

8.155 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 (e.g. 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.

8.156 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. Where a payment order can be revoked under regulations 83(3) or 83(4) of the PSRs 2017, a transaction must also be regarded as unauthorised after consent has been withdrawn.

8.157 The corporate opt out applies to regulations 67(3) and (4) of the PSRs 2017, 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)

8.158 Regulation 68 of the PSRs 2017 provides a mechanism whereby PSPs that issue card-based payment instruments that can be used to initiate a payment transaction from a payment 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).

8.159 Under regulation 68 of the PSRs 2017, CBPIIs can request confirmation from an ASPSP whether a customer has funds available in its payment account to complete a transaction at a given point in time. Regulation 68 of the PSRs 2017, however, 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~~

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.

8.160 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. We provide guidance on explicit consent in this context in **Chapter 17 – Payment initiation and account information services and confirmation of availability of funds**.
- 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 of the PSRs 2017.
- 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).

8.161 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, and therefore this is likely to mean real time.

8.162 On request by the customer, the ASPSP must inform the customer of the identity of the PSP which made the request for confirmation and the answer given.

8.163 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.

8.164 The ASPSP only has to provide confirmation where:

- The account is a payment account which is accessible online when the ASPSP receives the request (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 from that CBPII. As explicit consent is required before the first occasion on which a request is made, in our view, it is not required in respect of each individual request from the CBPII. The explicit consent obtained by the ASPSP must, however, relate to the specific CBPII making requests. 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 from any CBPII, nor would any form of "deemed" consent be acceptable. When a PSP receives a request for confirmation of availability of funds, it will need to

~~ensure that the request has been made by a CBPII in relation to which the customer has given their explicit consent.~~

ensure that the request has been made by a CBPII in relation to which the customer has given their explicit consent.

8.165 Regulation 68 of the PSRs 2017 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 (e.g. a gift card for a shopping centre). Account based e-money products would not be excluded from regulation 68 of the PSRs 2017.

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

8.166 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)

8.167 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)

8.168 Regulations 71(2) to (5) of the PSRs 2017 (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 Before blocking or stopping a payment instrument (e.g. a debit card or an e-banking ser vice), 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.

8.170 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 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. If, however, providing this information would compromise reasonable security measures, or would be unlawful (e.g. if it would constitute 'tipping off' under anti-money laundering legislation – see guidance at paragraph 19.20 in **Chapter 19 - Financial crime**), this requirement does not apply.

8.171 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 it cease to apply.

8.172 Where a payment instrument is blocked pursuant to regulation 71(2) of the PSRs 2017, and a PISP or AISP cannot access the customer's payment account as a result, this does not amount to a denial of access under regulations 71(7) – (10) of the PSRs 2017. See **Chapter 17 – Payment initiation and account information services and confirmation of availability of funds** for further details regarding denial of access.

8.173 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 set out

in the framework contract that spending limits may apply. This also does not affect the PSP from applying limits on types of transaction (such as limits imposed by the

in the framework contract that spending limits may apply. This also does not affect the PSP from applying limits on types of transaction (such as limits imposed by the relevant payment scheme), if set out in the framework contract that spending limits may apply.

Obligations of the customer in relation to payment instruments and personalised security details (regulation 72)

8.174 The customer is obligated by the PSRs 2017 to abide by the terms and conditions for the use of the payment instrument. A customer does not, however, 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.

8.175 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 of the PSRs 2017. Such terms may also be unfair under the CRA or UTTCRs.

8.176 The customer is obligated 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.

8.177 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.)

8.178 The PSRs 2017 also obligate 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 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.

8.179 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 8.174), 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)

8.180 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
- 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 of the PSRs 2017) to allow the customer to notify them if the

- have appropriate means available at all times (subject to the force majeure provisions of regulation 96 of the PSRs 2017) 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).

- be able to provide the customer on request with some way of proving that the customer has made the notification under regulation 72(1)(b) of the PSRs 2017 for 18 months after it has been made (e.g. 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).

- provide the customer with a way to notify the PSP 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.

8.181 PSPs must maintain adequate security measures to protect the confidentiality and integrity of customers' personalised security credentials in line with regulation 100(3) of the PSRs 2017 and SCA-RTS Article 22. SCA-RTS Articles 23 to 27 set specific requirements concerning the creation and transmission of credentials and their secure association with the payment service user, as well as the delivery and renewal of credentials, authentication devices and software and subsequent destruction, deactivation or revocation. 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)

8.182 The notification requirements relating to unauthorised transactions in regulation 74 of the PSRs 2017 do not apply in circumstances where a payment service is provided in relation to payment transactions that consist of the placing, transferring or withdrawal of funds covered by a credit line provided under a regulated agreement. See paragraph 8.141 for further details.

8.183 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.

8.184 In light of this, and in line with the obligation to provide information under paragraph 5(e) of Schedule 4 of the PSRs 2017, 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). Where a customer notifies a PISP rather than its ASPSP, the PISP may provide a refund directly to the customer if it wishes to do so. If it does not wish to provide a refund, we would expect the PISP to refer the customer to the ASPSP.

8.185 It should be noted that PSPs have the ability to grant more favourable terms to their customers, and therefore to offer a longer period (e.g. the UK Direct Debit Guarantee Scheme would not be prevented from continuing to offer a longer period for refunds).

8.186 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.

8.187 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)

8.188 Where the customer denies that they have authorised a payment transaction (e.g. claims that a card transaction was not made by them), or claims that a payment transaction has not been correctly executed (e.g. 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

8.189 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

8.190 We consider any parts of the transaction over which the PISP has control to be within its "sphere of competence".

8.191 The PSRs 2017 specifically provide that, just because the customer's payment instrument has been recorded by the PSP (including a PISP, if applicable) 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.

8.192 The effect of this is that, for all customers, other than businesses above micro-enterprise level and charities above small charity level (see **Glossary of Terms**) 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 ef fective 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.

8.193 Where a PSP (including a PISP, if applicable) claims that a customer has acted fraudulently or failed with intent or gross negligence to comply with its obligations under regulation 72 of the PSRs 2017, the PSP must provide supporting evidence to the payer. The evidence to be provided will depend on the circumstances of the case, but will not require the PSP to disclose evidence or information which the PSP is not permitted to disclose by law due to, for example, anti-money laundering legislation.

8.194 Regulation 75 of the PSRs 2017 applies in circumstances where a payment service is provided in relation to payment transactions that consist of the placing, transferring or withdrawal of funds covered by a credit line provided under a regulated agreement 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.

8.195 Under the Consumer Credit Act 1974, customers cannot be held liable for an unauthorised transactions on the basis of gross negligence. As such, references to gross negligence in regulation 75 of the PSRs 2017 would not be applicable where a payment service is provided in relation to payment transactions that consist of the placing, transferring or withdrawal of funds covered by a credit line provided under a regulated agreement.

8.196 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 (e.g. 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.)

8.197 The corporate opt out applies to this provision (see under 'General' at the start of Part II of this chapter).

PSP's liability for unauthorised transactions (regulation 76)

8.198 If a payment service is provided in relation to funds covered by a credit line provided under an agreement regulated by the CCA then regulations 76(1) – (4) of the PSRs 2017 will not apply and consumer credit provisions will apply instead. See paragraph 8.141 for further details.

8.199 For CCA regulated credit cards the PSP must apply the consumer credit regime to all unauthorised transactions instead of regulations 74, 76(1)-(4) and 77(1)-(5) of the PSRs 2017 (although regulation 75 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.

8.200 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.

8.201 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 (i.e. refund any charges and any interest which the customer has paid and/or credit interest which the customer has lost).

8.202 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.

8.203 A transaction should be treated as unauthorised unless the PSP has the consent of the customer as set out in regulation 67 of the PSRs 2017. 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.

8.204 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. Unauthorised transactions, however, 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).

8.205 The obligation to provide a refund is subject to any responsibility which the customer may have for the unauthorised transaction under regulation 77.

8.206 A refund must be provided to the customer as soon as practicable and in any event 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, in any event, by the end of Tuesday). The only exception to this is where the PSP has reasonable grounds for suspecting fraudulent behaviour by the customer 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.

8.207 The effect of this is that, in cases where PSPs do not have reasonable grounds to suspect fraudulent behaviour by the customer (e.g. 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.

8.208 It is not appropriate for the PSP to purport to make a refund for an unauthorised transaction conditional on the customer signing a declaration.

8.209 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.

8.210 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. This does not, however, require a PSP to provide a refund where it is prohibited from doing so by law or by anybody that it has notified under section 333A(2) of the Proceeds of Crime Act 2002.

8.211 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.

8.212 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 (e.g. 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).

8.213 Where an unauthorised, non-executed or defectively executed transaction is initiated through a PISP, it is the ASPSP's responsibility to provide a refund in line with regulation 76 and regulation 93 of the PSRs 2017 and this guidance. If the PISP is liable under regulation 76 or regulation 93 of the PSRs 2017, 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. We note that PSPs may put in place voluntary arrangements for the settlement of such liabilities between themselves.

8.214 Where an ASPSP has been required to compensate the customer for an unauthorised transaction under regulation 76 of the PSRs 2017, but that liability is attributable to an AISP, the ASPSP may exercise its right of recourse to seek compensation from the AISP (see paragraph 8.322).

8.215 Where a customer experiences detriment, other than in relation to an unauthorised or misdirected payment, as a result of a service provided by an AISP, the customer should, in the first instance, complain to the AISP and escalate any issues to the Financial Ombudsman Service (See Chapter 11 – Complaint Handling).

8.216 PSPs are at liberty to offer increased protections to customers in relation to unauthorised transactions and other areas, e.g. 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 obligated to provide under the PSRs 2017.

Customer's liability for unauthorised payment transactions (regulation 77)

8.217 If a payment service is provided in relation to funds covered by a credit line provided under a regulated agreement then regulations 77(1) – (5) of the PSRs 2017 will not apply and consumer credit provisions will apply instead. See paragraph 8.141 for further details.

8.218 A PSP 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. This does, however, 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, e.g. an outsourced provider

8.219 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 (e.g. if it was used anonymously) (see Part I, Section A of this chapter for a definition of low value payment instrument).

8.220 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 of the PSRs 2017 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 of the PSRs 2017 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.

8.221 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.

8.222 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 of the PSRs 2017)

- where the application of strong customer authentication was required pursuant to regulation 100 of the PSRs 2017 but the payer's PSP does not require it

- 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).

8.223 Where regulation 100 of the PSRs 2017 requires the application of strong customer authentication but the payee (e.g. the merchant) or the payee's PSP (e.g. the merchant acquirer) does not accept it, 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 the payer's PSP providing a refund to the customer. We expect the payee or payee's PSP to provide the refund within a reasonable period. The payer's PSP has a right of action in respect of this refund (regulation 148(4) of the PSRs 2017). **Chapter 20 – Authentication** provides further information regarding the application of strong customer authentication.

8.224 The corporate opt out applies to this provision (see under "General" at the start of this section).

Payment transactions where the transaction amount is not known in advance (regulation 78)

8.225 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.

8.226 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 payment account unless the customer has authorised the exact amount of funds to be blocked.

8.227 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.

8.228 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) of the PSRs 2017 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. We still, however, expect PSPs to take a reasonable approach to releasing funds and to do so as soon as possible. This may involve releasing funds in accordance with existing industry practice and the card schemes rules.

8.229 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)

8.230 This provision relates to payment transactions that have been initiated by or through the payee (e.g. debit or credit card transactions or direct debits), where the exact amount of the transaction was not specified at the point of authorisation (e.g. a variable-amount direct debit or card-based continuous payment authority, 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.

8.231 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.

8.232 The corporate opt out applies to this provision (see under "General" at the start of Part II).

8.233 For direct debit transactions which fall within the scope of the Regulation (EU) 260/2012 (i.e. SEPA direct debits), the payer is entitled to an unconditional refund from its PSP of the full amount of any direct debit transaction.

8.234 PSPs can agree more favourable terms with their customers (e.g. under the UK Direct Debit Scheme).

Requests for refunds for payment transactions initiated by or through a payee (regulation 80)

8.235 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. PSPs may, however, 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.

8.236 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.

8.237 The corporate opt out applies to this provision (see under "General" at the start of Part II of this chapter).

Execution of payment transactions

Receipt of payment orders (regulation 81)

8.238 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

8.239 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.

8.240 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).

8.241 In our view, an exception to this can be made where a promise or guarantee of payment has been given by the payer's PSP to the payee, e.g. in the case of pre-authorisation of card-based payment transactions where the amount is not known in advance (see regulation 78 of the PSRs 2017). In such cases it may be acceptable, on the basis of recital 77 to PSD2 and provided the PSP has complied with the requirements of regulation 78 of the PSRs 2017, for the funds to be earmarked pending receipt of the actual payment order.

8.242 Without such a promise or guarantee to the payee (e.g. 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 (e.g. 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) of the PSRs 2017.

8.243 The payer's PSP must not debit the customer's payment account before the receipt of a payment order.

8.244 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 (e.g. 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) of the PSRs 2017 regarding customer agreement will apply. PSPs should also take note of paragraphs 8.240 and 8.242 in respect of "earmarking".

8.245 In exceptional circumstances where, in spite of all efforts, it is not possible for 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 of the PSRs 2017 (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 allow refusal on these grounds. We would not expect that any such refusal would attract a charge.

8.246 It is expected that PSPs will have made the necessary arrangements to enable their customers to receive payments within the one business day timescale. Any PSP whose customer accounts are not reachable by Faster Payments, however, 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)

8.247 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 (e.g. 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.

8.248 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 (e.g. 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 (e.g. 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 (e.g. online) at the earliest opportunity and no later than the end of the next business day following receipt of the payment order.

8.249 Notification need not be provided for low value payment instruments if the non-execution is apparent from the context (e.g. the purchase is refused at point of sale) (see Part I, section A of this chapter for a definition of low value payment instrument).

8.250 If the refusal is reasonably justified and the framework contract so allows, the PSP may levy a charge for the refusal (unless the circumstance set out in paragraph 8.245 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 refusal in the framework contract and separately charge this to the underlying account.

Revocation of a payment order (regulation 83)

8.251 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 this 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)) of the PSRs 2017) 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 of the PSRs 2017 to an immediate refund from their PSP. It is best practice,

however, 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.

8.252 For other types of payments and for payment orders initiated by a PISP or by or through the payee (e.g. 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 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.

8.253 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.

8.254 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.

8.255 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.

8.256 For payment orders made direct by the payer to their PSP, revocation later than the limits set out in regulation 83 of the PSRs 2017 may be agreed with the relevant PSP or providers. For payment orders initiated by or through the payee (e.g. 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).

8.257 A charge may be made for revocation, if agreed in the framework contract.

8.258 The corporate opt out applies to this provision (see under "General" at the start of Part II of this chapter).

8.259 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)

8.260 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.

8.261 The payee can agree with its 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)

8.262 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

8.263 For all other types of transactions, the requirements will apply unless the PSP and its customer agree otherwise (but see also regulation 86(3) of the PSRs 2017). 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)

8.264 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').

8.265 An extra day may be added to the above period when the payment order is initiated in paper, rather than electronic form.

8.266 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. 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.

8.267 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.

8.268 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 4**.

8.269 While other models of acquiring may be possible, 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 our view that the contract between the merchant and the merchant acquirer to which the definition refers involves the execution of payment transactions. Adoption of a particular business model should not deprive PSD2 of its utility in achieving the protection of merchants who receive transfers of funds from acquirers, as referred to in recital 10 of PSD2. Therefore acquirers should ensure their customers receive the protection envisaged by PSD2 – in particular with respect to safeguards in the event of the acquirer's insolvency, execution times and information requirements.

8.270 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 of the PSRs 2017. See paragraphs 8.279 to 8.288 for further details.

8.271 For low value payment instruments, the PSP can agree with the customer that the execution times in regulation 86 of the PSRs 2017 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)

8.272 Where the payee does not hold a payment account with the PSP (e.g. 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".

8.273 For low value payment instruments, the PSP can agree with the customer that the execution times in regulation 87 of the PSRs 2017 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)

8.274 Cash placed by a consumer, micro-enterprise or small charity (see **Glossary of Terms**) 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. For other customers an extra business day is allowed. The requirements in regulation 88 of the PSRs 2017 only apply if the account is denominated in the same currency as the cash.

8.275 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.

8.276 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 PSP 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.

8.277 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 (e.g. 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 (e.g. 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 of the PSRs 2017.

8.278 Where a discrepancy in a cash deposit is discovered after the funds have been credited (e.g. 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)

8.279 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.

8.280 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.

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. We expect, however, 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.

8.281 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 PSP's 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.

8.282 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 a business day. A PSP must also not, 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. 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.

8.283 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".

8.284 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. The requirement for "immediate" availability, however, 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 (and whether the payment is received outside of business hours must be considered in accordance with paragraphs 8.281 – 8.283).

8.285 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.

8.286 Where a PSP is using its own internal processes to execute the transfer (i.e. 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.

8.287 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.

8.288 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 4**).

Liability

Incorrect unique identifiers (regulation 90)

8.289 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 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.

8.290 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.

8.291 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.

8.292 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 between PSPs could involve participating in industry arrangements relating to the recovery of funds (such as the credit payment recovery process).

8.293 If the payer's PSP is unable to recover the funds and the customer provides a written request, the PSP must, under regulation 90(4) of the PSRs 2017, provide to the customer all available relevant information in order for the payer to file a legal claim for repayment of the funds.

8.294 We would expect the relevant information provided pursuant to regulations 90(3) and (4) of the PSRs 2017 to include the payee's name and an address at which documents can be effectively served on that person. When providing information to its customers to ensure fair and transparent processing of personal data (e.g. in a privacy notice), as required by applicable data protection legislation, a PSP should take account of its potential obligations under regulations 90(3) and (4) of the PSRs 2017.

8.295 We would also consider it best practice for the payer's PSP, after receiving the relevant information from the payee's PSP but before providing such information to the payer under regulation 90(4) of the PSRs 2017, to notify the payee that this information will be provided to the payer.

8.296 In some cases of 'authorised push payment (APP) fraud' the payer intends to transfer the funds to a legitimate payee, but is deceived into providing the account number and sort code of an account held by a different person, and so transfers the funds to a fraudster. In our view, this is also provision of an incorrect unique identifier and PSPs must cooperate and make reasonable efforts to assist the payer in recovering the funds as required under regulation 90 of the PSRs 2017.

8.297 PSPs are under an obligation to comply with legal requirements to deter and detect financial crime as detailed in **Chapter 19 – Financial Crime**.

Non-execution or defective or late execution of payment transactions initiated by the payer (regulation 91)

8.~~296~~298 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.~~297~~299 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.~~298~~300 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.~~299~~301 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.~~300~~302 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.~~301~~303 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.~~302~~304 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.~~303~~305 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 of the PSRs 2017.

8.~~304~~306 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.~~305~~307 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.

8.~~306~~ 308 The corporate opt out applies to this provision (see under "General" at the start of Part II of this chapter).

Non-execution or defective or late execution of payment transactions initiated by the payee (regulation 92)

8.~~307~~309 This provision covers situations where the payment order has been initiated by the payee (e.g. credit or debit card payments, or direct debits), and the instruction has either not been carried out or carried out incorrectly.

8.~~308~~310 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.

~~**8.309** If it has failed to do this it must immediately re-transmit the payment order. The payee's PSP must also ensure that the transaction is handled in accordance with regulation 89 of the PSRs 2017 so that the amount of the transaction is at the payee's disposal immediately after it is credited to the payee's PSP's account and 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.~~

~~**8.310** 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.~~

~~**8.311** If the payer's PSP is liable, its liability is to its own customer rather than the payee, and it must, immediately, and as appropriate:~~

- ~~refund the payer the amount of the payment transaction (e.g. if the payer's account 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~~

~~**8.312** When it is restoring the payer's payment 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.~~

~~**8.313** 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~~

8.311 If it has failed to do this it must immediately re-transmit the payment order. The payee's PSP must also ensure that the transaction is handled in accordance with regulation 89 of the PSRs 2017 so that the amount of the transaction is at the payee's disposal immediately after it is credited to the payee's PSP's account and the credit value date is no later than the date ~~that~~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.

8.312 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.

8.313 If the payer's PSP is liable, its liability is to its own customer rather than the payee, and it must, immediately, and as appropriate:

- refund the payer the amount of the payment transaction (e.g. if the payer's account 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

8.314 When it is restoring the payer's payment 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.

8.315 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.

8.316 As with regulation 91 of the PSRs 2017, 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.~~315~~317 This may involve the refunding of charges and adjustment of interest. The ef fect 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.~~316~~318 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.~~317~~319 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 payment account to the state it would have been in if the defective payment transaction had not taken place.

8.~~318~~320 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. In this regard, the ASPSP has a right of action against the PISP (see paragraph 8.322 below). We note that PSPs may agree arrangements for the settlement of such
liabilities between themselves.

8.~~319~~321 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.~~320~~322 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 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.~~321~~323 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) and right of action (regulation 148)

8.~~322~~324 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 attributable to another PSP or an intermediary, the other PSP or intermediary must compensate the first PSP. This includes compensation where any of the PSPs fail to use strong customer authentication where it is required pursuant to regulation 100 of the PSRs 2017.

8.~~323~~325 In these circumstances, the first PSP also has a right of action against the other PSP. This entitles the first PSP to bring an action against the other PSP for compensation through the courts on the basis of the other PSP's failure to compensate the first PSP under regulation 95 of the PSRs 2017 (regulation 148(4) of the PSRs 2017).

Force majeure (regulation 96)

8.~~324~~326 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 of the PSRs 2017) 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 (e.g. anti-money laundering legislation)

Consent for use of personal data (regulation 97)

8.~~325~~327 Regulation 97 of the PSRs 2017 states that a PSP must not access, process or retain any personal data for the provision of payment services by it unless it has the explicit consent of its customer to do so. Data protection law, including the General Data Protection Regulation (GDPR) (EU 2016/679), may require a PSP to obtain a data subject's explicit consent (or satisfy another condition) to process any personal data classified as "sensitive personal data" under current data protection law or a "special category" under the GDPR.

8.~~326~~328 In respect of contracts entered into before 13 January 2018, if a PSP complies with its obligations under data protection law including the GDPR, we would not, as a matter of course, consider taking regulatory or disciplinary action against the PSP for breach of regulation 97 of the PSRs 2017 alone. PSPs should, however, refer to the Information Commissioner's guidance for more information on sensitive/special categories of personal data and the obligations under data protection law that might apply when processing them.

8.~~327~~329 In our view, regulation 97 of the PSRs 2017 does not permit an ASPSP to require explicit consent where it has an obligation to disclose information under other provisions of the PSRs 2017. For example, the ASPSP should not require explicit consent from its customer before it complies with its obligations under regulations 69 and 70 (relating to giving payment account data to AISPs or PISPs) or from its customer before complying with its obligations under regulation 90(3) of the PSRs 2017 (relating to misdirected payments).

Management of operational and security risks (regulation 98) and incident reporting (regulation 99)

8.330 Under regulation 98 of the PSRs 2017, PSPs must establish a framework, with appropriate mitigation measures and control mechanisms, to manage the operational and security risks relating to the payment services they provide and must also provide the FCA, on at least an annual basis, with an updated and comprehensive assessment of those risks. As part of the framework, PSPs must establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents. **Chapter 18 – Operational and security risks** and **Chapter 13 – Reporting and notifications** contain more information.

Authentication (regulation 100)

8.331 From 14 September 2019, all PSPs must comply with regulation 100 of the PSRs 2017 and with SCA-RTS.[34] **Chapter 20 – Authentication** provides further information.

8.332 Under regulation 100(3) of the PSRs 2017, PSPs must maintain adequate security measures to protect the confidentiality and integrity of payment service users' personalised security credentials. SCA-RTS Articles 22 to 27 specify the requirements, which include the creation and transmission of credentials and their secure association

34 The Commission Delegated Regulation (EU) 2018/389 (the SCA-RTS) is available here https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN

with the payment service user, as well as the delivery and renewal of credentials, authentication devices and software, and subsequent destruction, deactivation or revocation.

Part III: Additional conduct of business requirements for e-money issuers

8.~~328~~333 This section includes some additional conduct of business rules applicable to all e-money issuers, including those authorised under FSMA. They apply to the issuance and redemption of e-money carried on from an establishment in the UK.

8.~~329~~334 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.~~330~~335 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.~~331~~336 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.~~332~~337 Regulation 39 of the EMRs 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.~~333~~338 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.~~334~~339 Under the EMRs, e-money holders have the right to redeem the monetary value of their e-money (i.e. 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 of the EMRs).

8.~~335~~340 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 of the EMRs 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.~~336~~341 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.~~337~~342 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.~~338~~343 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.~~339~~344 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.~~340~~345 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.~~341~~346 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.~~342~~347 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.~~343~~348 The above guidance on redemption does not apply to a person (other than a consumer) who accepts e-money (e.g. 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.~~344~~349 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 sets out how authorised payment institutions (PIs), authorised e-money institutions (EMIs), and small EMIs should use their capital resources to meet their initial and ongoing capital requirements. It is not relevant to small PIs or registered account information service providers (RAISPs). The professional indemnity insurance (PII) requirements that will apply to firms carrying on account information services (AIS) and payment initiation services (PIS) are covered in **Chapter 3 – Authorisation and registration**. This chapter covers:

- Part I: Capital requirements for authorised PIs
  - Introduction
  - Initial capital requirements
  - Ongoing capital requirements
- Part II: Capital requirements for authorised EMIs and small EMIs
  - Introduction
  - Initial capital requirements
  - Ongoing capital requirements
- Part III Capital resources for authorised PIs, authorised EMIs and small EMIs

Part I: Capital requirements for authorised PIs

Introduction

9.2 The Payment Services Regulations 2017 (PSRs 2017) set out initial and ongoing capital requirements for authorised PIs. Under the PSRs 2017, 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: (i) initial capital requirements (which are a condition of authorisation); and (ii) 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.[~~29~~35]

9.6 Authorised PIs can undertake activities that are unrelated to providing payment services. These firms are called 'hybrid' firms. The PSRs 2017 do not impose any initial or ongoing capital requirements in relation to business carried on by such firms that does not involve payment services. Any other capital requirements imposed because of other legislation have to be met separately and cumulatively (e.g. if the authorised PI is undertaking an activity regulated under the Financial Services and Markets Act 2000 (FSMA)). Where the authorised PI carries out activities other than providing payment services, it must not include in its capital calculation any items used in carrying out those 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 applicant 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 it carries out (see table below). Where more than one initial capital requirement applies to the authorised PI, it must hold the greater amount.

9.8 The minimum initial capital required is as follows:

Payment Services (see Schedule 1 of 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 in (paragraphs 1 (a) to (e) of Part 1, Schedule 1 of the PSRs 2017)	€125,000

Ongoing capital (or 'own funds') requirements for PIs

9.9 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 that is required for its business activity; or
- the amount of the own funds requirement calculated in accordance with method A, B or C (described below), subject to any adjustment we require.

29

35 Current and historical rates can be found on the European Commission's InforEuro website.

9.10 The ongoing capital held must not fall below the level of the initial capital requirement for the services provided. This differs, however, for:

- authorised PIs that are included within the consolidated supervision of a parent credit institution pursuant to the Capital Requirements ~~Directive[30]~~Directive[36] and where all of the conditions specified in Article 7(1) of the Capital Requirements ~~Regulation[31]~~Regulation[37] have been met; and

- authorised PIs that carry on PIS only.

Unlike other authorised PIs, these firms are simply required to continue to hold the amount of initial capital required for their business activities at all times.

Calculation of ongoing capital (or 'own funds') requirements for PIs

9.11 This section explains the three calculation methods the different own funds requirements: methods A, B and C.

9.12 The applicant will be asked, in the authorisation application pack, to indicate which calculation method it wishes to use. Ultimately, however, we will direct which method it must use. We will do this based on our evaluation of the applicant firm, taking into account its preference as stated in the application pack.

Method A

9.13 Method A is based on the firm's fixed overheads. The calculation is normally 10% of the firm's fixed overheads in the previous financial year. If, however, there is a material change in the firm's business since the previous financial year, we may decide that the requirement is higher or lower than 10%. Examples of a material change include the sale of parts of the firm, a business acquisition and rapid growth (typically of a new firm).

9.14 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

9.15 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 at paragraph 9.18 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 firm's payment transactions executed in the previous financial year divided by the number of months in that year and scaled in the following manner:

~~30~~36 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').

~~31~~37 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').

- 4% of the slice of the average monthly payment volume up to €5 million;
- 2.5% of the slice of the average monthly payment volume above €5 million up to €10 million;
- 1% of the slice of the average monthly payment volume above €10 million up to €100 million;
- 0.5% of the slice of the average monthly payment volume above €100 million up to €250 million; and
- 0.25% of the average monthly payment volume above €250 million.

Method C

9.16 Method C is based on the firm's income over the previous financial 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. This is the sum of the firm's interest income, interest expenses, commission and fees received as well as other operating income, defined as follows:

- 'interest income: interest received by the authorised PI from the investments it has made whether or not made from 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 of the PSRs 2017) – these should be expressed in gross

9.17 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.

9.18 The scaling factor applied to methods B and C is based on the type of service provided, and is the greater 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 (as specified in paragraphs 1(a) to (e) of Part 1, Schedule 1 of the PSRs 2017)	1.0

9.19 When calculating the ongoing capital requirement, if the authorised PI has not completed a financial year of business, references to the figure for the preceding f inancial year should be taken as the projected figure which it used in the business plan submitted as part of its application for authorisation (subject to any adjustments that we may have required).

9.20 We may direct an authorised PI 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, based on our evaluation of the firm. Our 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

9.21 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.

9.22 The exception is where the PSRs 2017 provide for a different method of recognition, measurement or valuation.

Part II: Capital requirements for authorised EMIs and small EMIs

Introduction

9.23 The Electronic Money Regulations 2011 (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**.

9.24 The term 'capital resources' describes what a business holds as capital.

9.25 The term 'capital requirements' refers to the amount of capital that must be held by the business for regulatory purposes. The EMRs establish: (i) initial capital requirements (which 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. EMIs 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.

9.26 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 unrelated payment services. This will primarily be relevant where the authorised EMI provides payment services that are independent from its e-money products. Where an authorised EMI simply transfers funds from e-money accounts, such as where a customer uses their e-money to pay a utility bill, this payment service would relate to the activity of issuing e-money.

9.27 Additionally, EMIs can undertake activities that are unrelated to issuing e-money and providing payment services. These firms are called 'hybrid' firms. The EMRs do not impose any initial or ongoing capital requirements in relation to the business carried on by a hybrid firm that does not involve issuing e-money or providing payment services. Any other capital requirements imposed by other legislation have to be met separately and cumulatively (e.g. if the EMI is undertaking an activity regulated under FSMA).

9.28 For the purposes of calculating the capital requirements, EMIs that provide unrelated payment services or that are hybrid firms must treat each part of the business separately.

Initial capital requirements for EMIs and small EMIs

9.29 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.

9.30 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.

9.31 If the applicant for small EMI status does not have a sufficient period of business history to calculate average outstanding e-money, they may use projected amounts as outlined in their business plan, subject to any adjustments that we may require.

9.32 The items that may be used to meet the initial capital requirement are set out in part III of this chapter.

Ongoing capital (or 'own funds') requirements

E-money issuing business

9.33 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 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 that we may require).

9.34 The ongoing capital held must not fall below the level of the initial capital requirement for the services provided.

9.35 Small EMIs that are 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

9.36 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.

9.37 The ongoing capital requirements for unrelated payment services are laid out in paragraph 13(a) of Schedule 2 of the EMRs and correspond to methods A, B and C as detailed in paragraphs 9.11 – 9.22.

9.38 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 firm) which method the firm must use, taking into account its preference as stated in the application pack.

9.39 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.

9.40 Small EMIs are allowed to provide payment services unrelated 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.

Calculating ongoing capital ('own funds') requirements for e-money businesses

9.41 Descriptions of methods A, B and C (for the unrelated payment services business) are set out above. A description of method D (for the e-money business) is set out below.

9.42 Authorised EMIs that have not completed six months for the e-money business or a f inancial year for the unrelated payment services business should use the projected f igure submitted in their business plan in their application for authorisation (subject to any adjustments we may require).

9.43 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 firm. Our 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

9.44 Method D is 2% of the average outstanding e-money issued by the EMI.

9.45 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.

9.46 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 or registration (subject to any adjustments that we may have required).

9.47 If an authorised EMI provides payment services that are unrelated to issuing e-money or is a hybrid firm 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 our satisfaction. 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 may have been, required by us.

Applying accounting standards

9.48 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 of 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.

9.49 The exception is where the EMRs provide for a different method of recognition, measurement or valuation.

Part III: Capital resources for authorised PIs, authorised EMIs, and small EMIs

9.50 This Part is about which items (known as "capital resources") can be used to meet capital requirements.

Meeting initial capital requirements

9.51 Schedule 3 Part 1(1) of the PSRs 2017 and Schedule 2 Part 2 of the EMRs (as amended) set out the items that can be used by authorised PIs, authorised EMIs and small EMIs (as applicable) to meet initial capital requirements. Such firms may use one or more of the items specified in Article 26(1)(a) to (e) of the Capital Requirements Regulation. These items are:

- Capital instruments (e.g. ordinary shares)
- Share premium accounts
- Retained earnings
- Other comprehensive income
- Other reserves

9.52 An authorised PI, authorised EMI, or small EMI must not include in its capital calculations any item also included in the capital calculations of another authorised PI, EMI, credit institution, investment firm, asset management company or insurance undertaking within the same group. Also, where an authorised PI, authorised EMI or small EMI carries out activities other than providing payment services, it must not include in its capital calculation any items used in carrying out the other activities.

'Own funds' to meet ongoing capital requirements for authorised PIs, authorised EMIs and small EMIs

9.53 The ongoing capital requirement is to be met by the authorised PI, authorised EMI, or small EMI's capital resources, which is formed of own funds. The ongoing capital held must not fall below the level of the initial capital requirement for the services provided.

9.54 Regulation 2 of the PSRs 2017 and regulation 2 of the EMRs set out that own funds has the definition given in Article 4(1)(118) of the Capital Requirements Regulation. Own funds consist of Tier 1 and Tier 2 items. Tier 1 is formed of Common Equity Tier 1 and Additional Tier 1. At least 75% of Tier 1 capital must be held as Common Equity Tier 1 capital and Tier 2 capital must be equal to or less than one third of Tier 1 capital.

9.55 The process below shows how own funds can be calculated. We only include the relevant parts of the Capital Requirements Regulation that apply to authorised PIs, authorised EMIs, or small EMIs. We exclude those elements of the Capital Requirements Regulation that only apply to banks (e.g. those relating to internal ratings-based models). The flow chart should be used in tandem with the Capital Requirements Regulation and does not replace the Capital Requirements Regulation, which can be read on the EurLexwebsite.

Figure 1 – Overview of 'own funds'

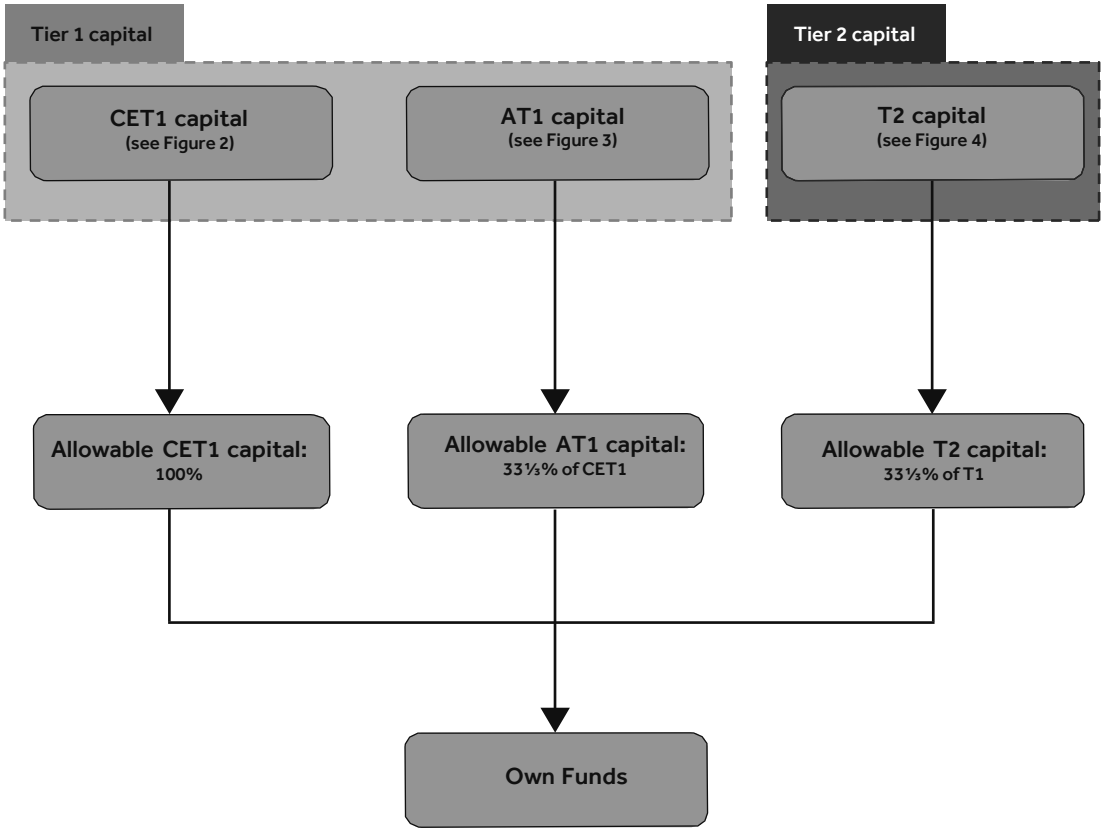


Figure 2 – Common Equity Tier 1 (CET1) capital

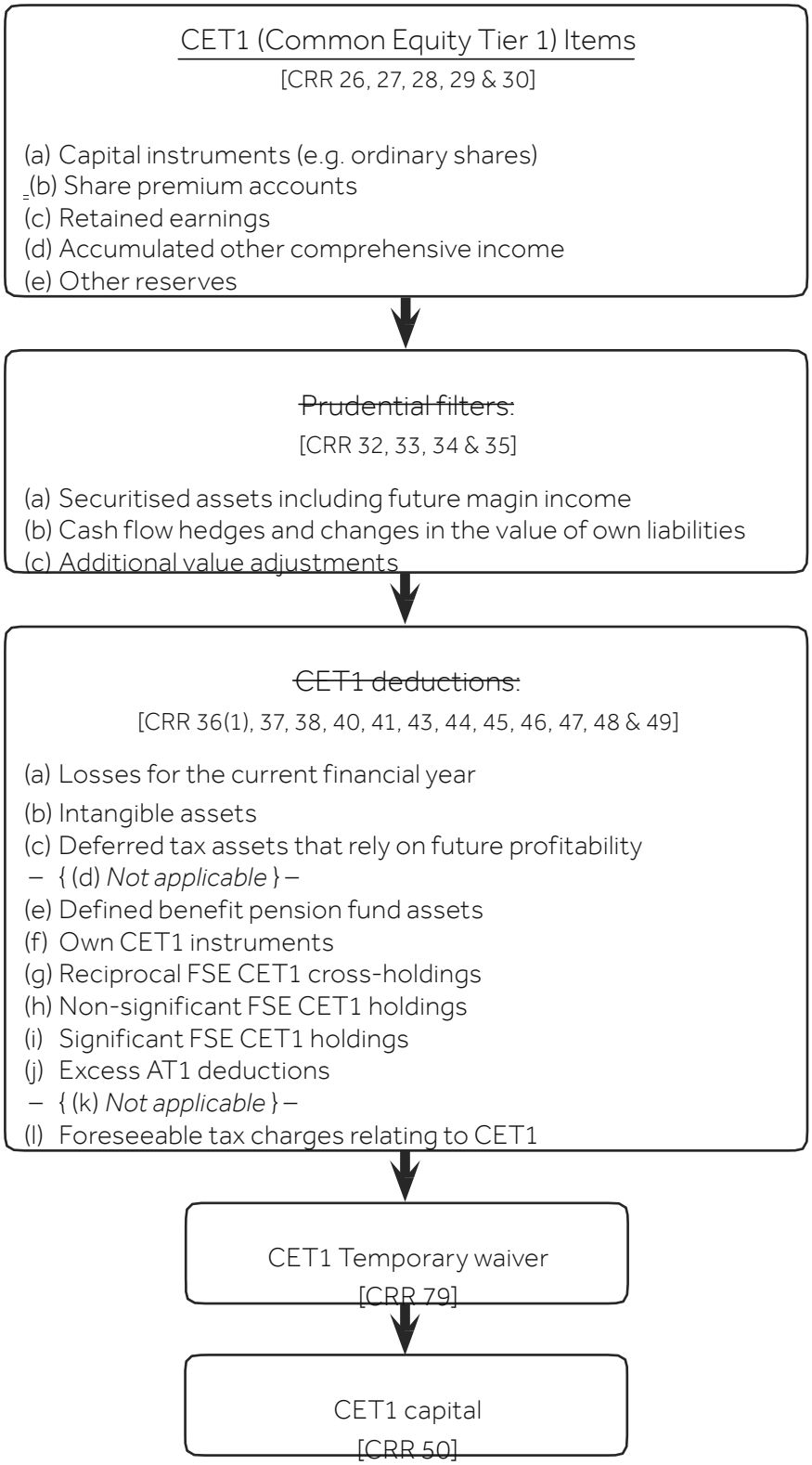


Figure 3 – Additional Tier 1 capital

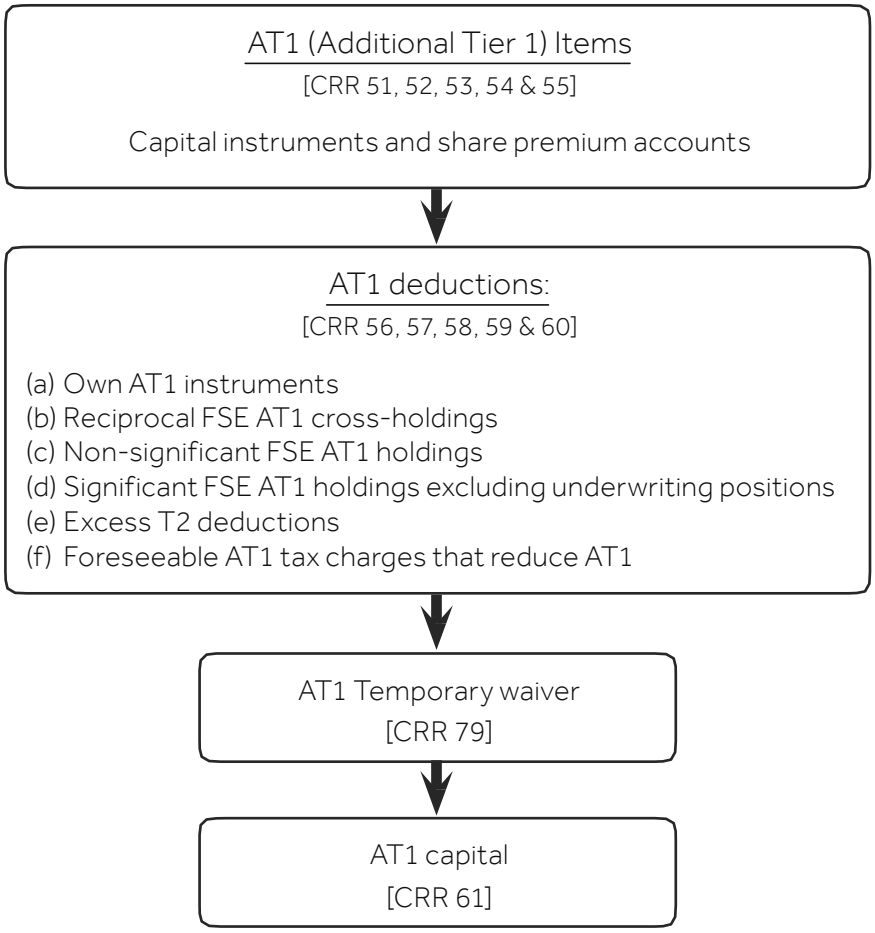
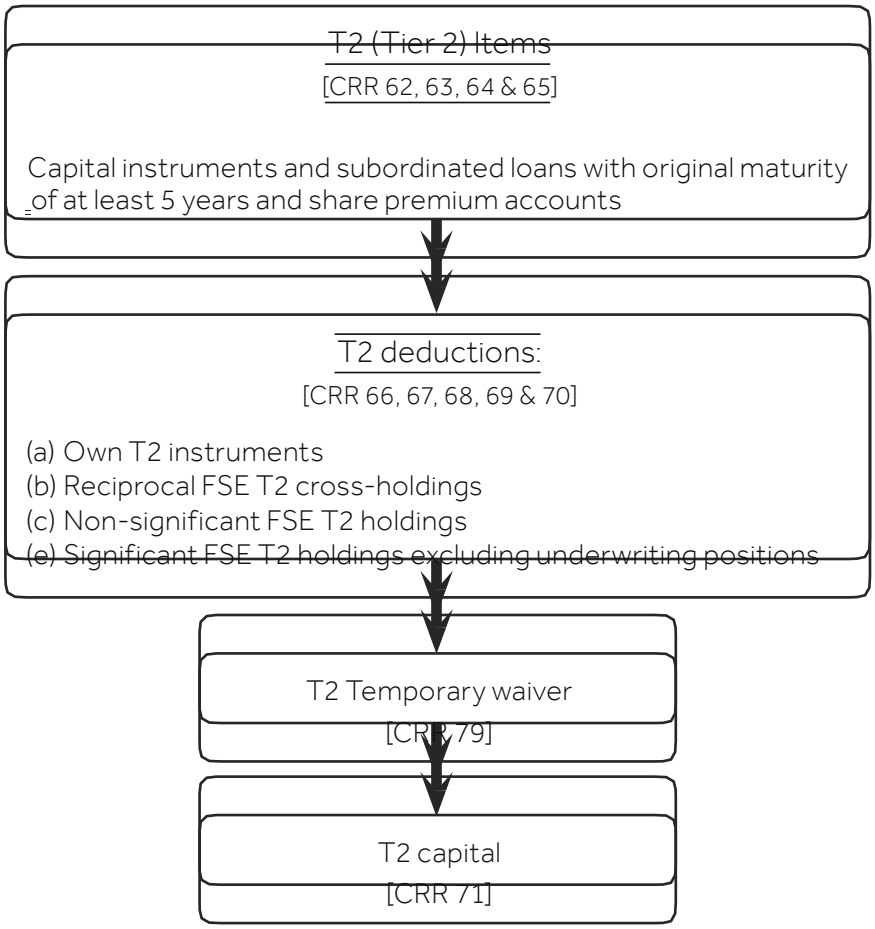


Figure 4 – Tier 2 capital



9.56 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

10 Safeguarding

Introduction

10.1 This chapter explains the safeguarding requirements for authorised payment institutions (Authorised PIs), authorised e-money institutions (Authorised EMIs), small e-money institutions (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 payment institutions (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 paragraphs 10.14 -10.17).

Safeguarding funds from payment services under the Payment Services Regulations 2017 (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 Electronic Money Regulations 2011 (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 the Financial Services and Markets Act 2000 (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 paragraph 10.14 to 10.17) 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 or 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 (PSP) 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, see paragraph 10.25 for when the safeguarding requirements apply. Examples include:

- an EMI with a foreign exchange business
- a foreign exchange business that also provides money transmission services
- a telecommunications network operator which receives funds from the public both for the provision of its own services (e.g. airtime) and for onward transmission to third parties.

10.19 The EMRs and PSRs 2017 safeguarding requirements only apply to relevant funds. Sometimes, however, 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 or 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 or 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 Q31K in PERG 13). The institution would thereby have to comply with the client money requirements in CASS 7 of the 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 European Economic Area (EEA) should note that transactions where both the payer and the payee are outside the EEA (e.g. 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. If, however, 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 institution's name, funds in an account in the institutions name at another institution and funds held on trust for the institution. See paragraphs 10.15 and 10.28 for more details regarding when we consider funds to have been received.

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 PSP. If a chain of PSPs is involved, an institution's safeguarding obligation continues while it holds the funds and ends when it has transferred them to another PSP which holds the funds on behalf of the payment service user. The funds must be safeguarded by the institution for the benefit of the payer or payee; it is not sufficient for the funds to be safeguarded for the benefit of another institution 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:

A. the segregation method

B. the insurance or comparable guarantee method

An institution may safeguard certain relevant funds using the segregation method and the remaining relevant funds using the insurance or comparable guarantee method. If an institution chooses to use both methods of safeguarding, it should be clear from the institution's records which funds are safeguarded using each method.

10.30 We expect institutions to notify us if they intend to change which method(s) they use to safeguard funds in line with their obligation to notify a change in circumstances under regulation 17 of the EMRs or regulation 37 of the PSRs 2017.

A. The segregation method

10.31 The first method requires the institution to segregate the relevant funds (i.e. to 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 or 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. This, however, increases risk to relevant funds. We expect institutions to segregate the relevant funds by moving them into a segregated account as frequently as practicable throughout the day. In the same way, where a customer incurs fees and the institution has a valid right to deduct the fees from the relevant funds it holds for that customer, any fees so deducted should be removed from the segregated account as frequently as practicable. 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 its agent or 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 (except in accordance with the provisions referred to in paragraph 10.42). An institution may safeguard some relevant funds using the segregation method, and other relevant funds using the insurance or comparable guarantee methods. If this is done, the same

account may be used both to hold properly segregated funds and to receive and hold

the proceeds of the relevant insurance policy or comparable guarantee, but must not be used to hold any other funds. For EMIs or 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. This will primarily be relevant where an EMI provides payment services that are independent from its e-money products. The requirement to separately safeguard funds will not apply where an EMI simply transfers funds from e-money accounts, such as where a customer uses their e-money to pay a utility bill.

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 21 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 (e.g. a right of set off) or interest (e.g. 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 Regulation 23(9) of the PSRs 2017 and regulation 21(4A) of the EMRs make provisions that are relevant to the safeguarding of relevant funds by an authorised PI or EMI that is a participant in a system that is designated for the purposes of the Financial Markets and Insolvency (Settlement Finality) Regulations 1999. It is possible for such participants to safeguard relevant funds, in accordance with these provisions, in an account with the Bank of England that the authorised PI or EMI holds for the purposes of completing settlement in the designated system.

10.43 The EMRs and PSRs 2017 do not prevent institutions from holding more than one safeguarding account.

10.44 The EMRs and 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.

10.45 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

10.46 Where an institution chooses to invest relevant funds into assets, regulations 23(6)b of the PSRs 2017 and 21(6)(b) 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.

10.47 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.

10.48 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.

B. The insurance or guarantee method

10.49 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 either all relevant funds (not just funds held by an institution at the end of the business day following the day that they were received) or certain relevant funds (with the remaining relevant funds protected by the segregation method, as above).

10.50 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.

10.51 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.

10.52 The proceeds of the insurance policy or comparable guarantee must be payable into a separate safeguarding account held by the institution. If the institution is using the insurance or comparable guarantee method to safeguard all relevant funds, the account must be used only for holding such proceeds. If an institution has decided to

use a combination of the two safeguarding methods, the account may also be used

for holding funds segregated in accordance with the segregation model. The account must be named in a way that shows that it is a safeguarding account rather than an account used to hold money belonging to the institution. 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).

10.53 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.

10.54 If EMIs or 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.

10.55 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)[32][38] to carry out non-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.

10.56 Neither the authorised credit institution nor the authorised insurer can be part of the corporate group to which the institution belongs.

Systems and controls

10.57 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(17) 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.

10.58 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.

10.59 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

~~32~~38 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

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 (e.g. 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

10.60 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(6) of the PSRs 2017 applies) held in a safeguarding account.

10.61 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).

10.62 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).

10.63 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.

10.64 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.

10.65 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.

10.66 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

10.67 If an insolvency event (listed in regulation 24 of the EMRs or regulation 23(18) 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.

10.68 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 Complaints handling

11.1 This chapter summarises the complaints handling requirements that apply to all payment service providers (PSPs), including banks, building societies, payment institutions (PIs), e-money money institutions (EMIs), registered account information service providers (RAISPs) and e-money issuers.

Introduction

11.2 Complaints handling covers three areas:

- how PSPs 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 PSP's/e-money issuer's response
- our role in handling complaints from customers and other interested parties about alleged breaches of the Payment Services Regulations 2017 (PSRs 2017) and the Electronic Money Regulations 2011 (EMRs), and about us

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 11.36.

11.5 All PSPs 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 PSPs 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 from non-eligible complainants about rights and obligations under Parts 6 and 7 of the PSRs 2017 are set out in regulation 101 of the PSRs 2017.

Providing information about complaints procedures

11.9 The PSRs 2017 require PSPs 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 an e-money issuer's business.

11.10 This means informing users about:

- the PSP's own complaints mechanism
- where the user will be an eligible complainant, the availability of the Financial Ombudsman Service
- where the user would not be an eligible complainant, the availability of another dispute resolution provider or an explanation that the PSP does not uses such services) and
- any other alternative dispute resolution procedures (such as under the Online Dispute Resolution Regulations (EU 524/2013))

11.11 Users must be informed 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'

11.12 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.

11.13 PSPs and e-money issuers are also subject to the consumer awareness rules in DISP 1.2 when dealing with complaints from eligible complainants. The information required under the PSRs 2017 can be provided using the summary details required under DISP 1.2. DISP 1.2 is modified to take account of the information requirements under the PSRs 2017.

11.14 The requirements for PSPs are therefore different in terms of content and timing from the requirements in DISP 1.2 for other types of business. For payment services business, eligible complainants must be referred to the availability of the information provided in accordance with paragraph 11.10 above, and at the branch where the ser vice is provided. For most other types of business, the PSP or e-money issuer should refer eligible complainants to the availability of these summary details at or immediately after the point of sale. 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.

11.15 This means PSPs 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, PSPs 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

11.16 Article 101 of PSD2 sets out time limits for handling complaints. For eligible complainants these are implemented by our rules in DISP. DISP 1.6.2A requires PSPs 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, where the respondent cannot send a final response within this period of time, for reasons beyond the control of the PSP, 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 DISP 1.6.2.

11.18 The definition of 'business day' for the purpose of calculating response time limits in DISP 1.6.2A for PSD complaints and EMD complaints reflects that in PSD2 and the PSRs 2017. When calculating response times, PSPs and e-money issuers must therefore consider whether this definition of 'business day' includes more calendar days than the standard Handbook definition of 'business day'.

11.19 PSPs 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.

11.20 If they want to, PSPs 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.

11.21 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).

11.22 For PSD complaints from complainants that are not eligible complainants, regulation 101 of the PSRs 2017 requires PSPs to respond to complaints within 15 business days or, in exceptional circumstances beyond the PSP's control, 35 business days. Regulation 101 of the PSRs 2017 also sets out the information requirements that apply in these circumstances.

Complaints recording and reporting

11.23 PSPs 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.

11.24 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 and PIs must follow the instructions on the GABRIEL system to submit their returns electronically. EMIs should download the payment services complaints form available here, complete it electronically in Excel, and send it to us by email to regulatory.reports@fca.org.uk.

11.25 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 of the PSRs 2017 as well as DISP 1) and to complaints from e-money holders that are eligible complainants.

11.26 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

11.27 The Financial Ombudsman Service operates the alternative dispute resolution (ADR) procedure for payment service users and e-money holders that are eligible complainants required by PSD2 and 2EMD.

11.28 The Financial Ombudsman Service is a statutory, informal dispute-resolution service, established under FSMA and independent of us. 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.

11.29 In deciding what is fair and reasonable in all the circumstances of a case the Financial Ombudsman Service will consider the relevant laws and regulations, the regulator's rules, guidance and standards, as well as codes of practice, and (where appropriate) what is considered to be good industry practice at the relevant time.

11.30 Where a PSP receives a complaint from a payment service user about rights and obligations under Parts 6 and 7 of the PSRs 2017, but that payment service user is not an eligible complainant, the PSP is required, if it uses dispute resolution services, to inform the payment service user of at least one provider of such services which is able

to deal with its complaint (regulation 101 of the PSRs 2017). 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 PSP has an agreement (if any such dispute resolution services are used).

Jurisdiction of the Financial Ombudsman Service

11.31 The Financial Ombudsman Service has two jurisdictions:

- The compulsory jurisdiction (CJ) covers financial businesses regulated by the PRA and FCA, certain other financial businesses registered with the FCA, activities specified in rules made by the FCA, and is mainly restricted to services provided in or from the UK.

- Financial businesses that are not covered by the CJ may volunteer to join the voluntary jurisdiction (VJ), which covers financial businesses that volunteer to join it, activities specified in rules made by the Financial Ombudsman Service with our approval, and services directed at the UK from the EEA, as well as services provided in or from the UK.

11.32 All PSPs 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.

11.33 Complaints can be made about PSPs and e-money issuers that no longer provide payment services or issue e-money. Former PSPs and former e-money issuers remain in the CJ for complaints about an act or omission that occurred when they provided payment services or issued e-money, as long as the CJ rules at the time the activity took place.

11.34 Further information about the Financial Ombudsman Service's processes for handling complaints is available on its website.

11.35 There is also information specifically for smaller businesses.

Eligible complainants

11.36 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 11.39)
- 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
- Consumer-buy-to-let (CBTL) consumers (in relation to CBTL business)

11.37 A business may not bring a complaint about an activity that it has permission to conduct itself. This extends to complaints from e-money issuers about payment ser vice provision, as all e-money issuers are also entitled to provide payment services.

11.38 If a PSP 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.

11.39 A micro-enterprise is a business which both:

- employs fewer than 10 people
- has a turnover or annual balance sheet that does not exceed €2 million

11.40 When calculating turnover or balance sheet levels, the European Commission's monthly accounting rate of the euro may be used.[~~33~~39]

11.41 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. PSPs 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. If this information is not easily available, however, the dual test would allow a complainant instead to rely on its status at the time of making the complaint.

11.42 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.

11.43 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. If, however, the complainant was not eligible at the time the complaint was made and the case appears to be 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

11.44 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

[~~33~~39] 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

1 November 2009 where the PSP was subject to the Financial Ombudsman Service's jurisdiction before that date.

Territorial scope of the CJ for complaints against PSPs and e-money issuers

11.45 The CJ 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

11.46 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 (VJ) of the Financial Ombudsman Service

11.47 The VJ covers financial businesses that volunteer to join it, covers activities specified in rules made by the Financial Ombudsman Service with our approval, and covers ser vices directed at the UK from the EEA, as well as services provided in or from the UK. It is available to PSPs, e-money issuers, and other financial businesses.

11.48 Firms, PSPs, and e-money issuers can join the VJ to allow consumers to take complaints to the Financial Ombudsman Service about acts or omissions before they joined the compulsory jurisdiction.

11.49 Firms that want to join the VJ should contact the Financial Ombudsman Service (see **Annex 2 – Useful Contact Details**).

Complaints to the FCA

11.50 We are required to maintain arrangements to enable payment service users, e-money holders and other interested parties, including, for example, consumer associations and PSPs) to submit complaints to us about PSPs' or e-money issuers' alleged breaches of the PSRs 2017 or EMRs. Information about how to complain can be found on our website.

11.51 Our process for dealing with these complaints is in accordance with the Guidelines on Procedures for Complaints of Alleged Infringements of Directive (EU) 2015/2366 issued by the EBA under Article 100(6) of PSD2.[~~34~~40]

[~~34~~40] https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-procedures-for-complaints-of-alleged-infringements-of-the-psd2

11.52 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

11.53 Anyone directly affected by the way in which we have exercised our 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.

12 Supervision

12.1 This chapter describes how we supervise payment service providers (PSPs) and e-money issuers under the Payment Services Regulations 2017 (PSRs 2017) and Electronic Money Regulations 2011 (EMRs). We also summarise our supervisory approach under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs).

Introduction

12.2 All PSPs and e-money issuers will be supervised in accordance with our general approach to supervision. More information is available on our ~~website~~[35] website[41], including details of how different types of firms are supervised and our responsibilities for prudential supervision. 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. Our 2017 Mission ~~document~~[36] document[42] explains our priorities in the regulation of the financial services sector. It provides the framework for the strategic decisions we make, the reasoning behind our work and the way we choose the tools to do it.

12.3 Our preference is to work in an open and cooperative relationship with all 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.[37] [43]

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 PSP or e-money issuer with a significant market presence as a " fixed portfolio firm". Fixed portfolio firms are subject to the highest level of super visory attention. We make it clear to a PSP or e-money issuer 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:

~~35~~

41 https://www.fca.org.uk/about/supervision

~~36~~42 https://www.fca.org.uk/publication/corporate/our-mission-2017.pdf

~~37~~43 See regulation 37 PSRs 2017, regulation 37 EMRs and Chapter 4 of the Approach Document (Change in circumstances of

authorisation).

- 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 payment institutions (PIs), registered account information service providers (RAISPs), and e-money institutions (EMIs), which include 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:

- 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, there is a breach of the requirements in the PSRs 2017. 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 European Banking Authority's (EBA) Guidelines on Procedures for Complaints of Alleged Infringements of Directive (EU) 2015/2366 developed under Article 100(6) of PSD2.[~~38~~44]

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

[~~38~~44] https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-procedures-for-complaints-of-alleged-infringements-of-the-psd2.

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 the Financial Services and Markets Act 2000 (FSMA) (Consumer redress schemes). Section 404 of FSMA allows us 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.[~~39~~45]

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 f inancing requirements of European Economic Area (EEA) authorised EMIs, PIs and RAISPs 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, EMI or RAISP's head office is situated in another EEA State and it operates in the UK through agents pursuant to the right of establishment, that PI, EMI or RAISP may be required to appoint a central contact point in the UK in order to facilitate the supervision of those networks of agents. The circumstances in which the appointment of a central contact point is appropriate and the functions of the contact point shall be determined in accordance with the Regulatory Technical Standards developed by the EBA under Article 29(5) of PSD2.

12.15 Under the PSRs 2017 and the EMRs we may direct that an EEA authorised PI or EMI or an EEA registered RAISP 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 or an EEA registered RAISP has exercised its right of establishment in the UK, to monitor compliance with Parts 6 and 7 of the PSRs 2017. The means details and frequency of reporting requested by host states will be specified by Regulatory Technical Standards developed by the EBA under Article 29(6) of PSD2.

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

[~~39~~45] https://www.fca.org.uk/publication/guidance-consultation/guidance10.pdf.

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; and

- 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 obligated under the PSRs 2017 and EMRs to report to us 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[40]~~links[46] 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 PI or EMI 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 MLRs apply to all PSPs and e-money issuers.

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

~~40~~46 'Close links' has a specific meaning in this context. Please refer to regulation 25 of the EMRs and regulation 24 of the PSRs.

by HM Treasury under the Counter-Terrorism Act 2008. **Chapter 19 – Financial Crime** contains further detail on our approach to financial crime.

12.24 We are 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";[41][47]
- EMIs;
- PIs other than those that have authorisation to provide money remittance payment services (see below); and
- RAISPs.

12.25 PIs, including "bill payment service providers"[42][48] that are authorised to provide money remittance services[43][49] only, are supervised for compliance with the MLRs by HMRC and need to register with HMRC accordingly.[44][50] PIs (including bill payment service providers) with permission to carry on money remittance and other, additional payment services may be supervised under the MLRs by either us or HMRC, depending on the nature of the regulated payment services activity carried out. In these cases, we 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 us under the MLRs to register separately as an Annex 1 Financial Institution. If you are currently registered with us as an Annex 1 Financial Institution you can apply to us to deregister to avoid additional fees.

12.27 We have 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 regulations 19(1) to (5) of the MLRs. We may include any PSP or e-money issuer in our thematic reviews.

12.28 All firms that we supervise can find helpful guidance on how to prevent financial crime in our FinancialCrime:AGuideforFirms.

---

[41][47] 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).

[42][48] As defined in regulation 3(1) of the MLRs.

[43][49] The activity listed at paragraph 1(f) of Part 1, Schedule 1 of the PSRs 2017.

[44][50] 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 Payment service providers (PSPs), e-money issuers and other businesses are required under the Payment Services Regulations 2017 (PSRs 2017) and the Electronic Money Regulations 2011 (EMRs) to provide certain data and information to us either periodically or under specified circumstances. In some cases we must provide this information in turn to HM Treasury, ~~the~~ European Commission, ~~the~~ European Banking Authority (EBA) or ~~the~~ European Central Bank (ECB).

13.2 **Chapter 4 – Changes in circumstances of authorisation or registration** covers the notifications that payment institutions (PIs), e-money institutions (EMIs) and registered account information service providers (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 ~~f irm~~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 Part I of this chapter deals with the periodic reports that are required under the PSRs 2017 and EMRs. Part II covers the event-driven notification requirements under the PSRs 2017 and the SCA-RTS.[51] 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, (including ASPSPs, AISPs and PISPs), e-money issuers and excluded providers.

51 The Commission Delegated Regulation (EU) 2018/389 (the SCA-RTS) is available here https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN

Part I: 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 (note there are some transitional provisions for the first reporting period following 13 January 2018 – see SUP TP 1.11).

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 authorisation 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, an 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 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 account information service (AIS) or payment initiation service (PIS) activity, the calculated minimum monetary amount of the professional indemnity insurance (PII) and whether the terms of the insurance policy held have changed in any material way since authorisation (to assess the continued suitability of the PII cover)

RAISPs are asked only 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 PII policy held have changed in any material way since authorisation (to assess the continued suitability of the PII cover)

Process

Authorised PIs and RAISPs should follow the instructions on the e-Gabriel online system to submit their returns electronically. Gabriel can also be used to view a tailored schedule of a particular authorised PI or RAISP's 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: Gabriel

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 HM Treasury with the necessary information so that it can report the total value of small PI payment transactions to the European Commission and further to assess whether the small PI has continued to meet the conditions for registration)
- the number of new 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

Small PIs 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 a particular small PI's reporting requirements.

Report required: FIN060 (EMI and SEMI Annual Return)

Required to submit: Authorised and small EMIs

Frequency: Annual

Submission date: Within 30 business days of the EMI's accounting reference date

(Note there are some transitional provisions for the first reporting period following 13 January 2018 – see SUP TP 1.11)

Method of submission: Email

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 questionnaire), 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 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 professional indemnity 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~~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

Authorised and small EMIs should download the applicable EMI returns available here, complete them electronically in Excel, and send them to us by email to: regulatory.reports@fca.org.uk.

Report required: FSA065 Total outstanding e-money at 31 Dec

~~**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 HM 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 us to meet our obligation in providing the requisite information to HM Treasury.

Process

Small EMIs should download form FSA065 available here complete it electronically in Excel, and send it to ~~us by email~~ us 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 European Economic Area (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: Email

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

E-money issuers submitting information on average outstanding e-money should contact ~~regulatory.reports@fca. org.u~~regulatory. reports@fca.org.uk for more information about the method of submission.

Report required – DISP 1 Annex 1AD Payment services and electronic money complaints report

Required to submit: All PSPs (credit institutions, PIs, EMIs and RAISPs)

Frequency: Annual

Submission date: Within 30 business days of a 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: Gabriel (email if EMI)

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 2017.

Process

All PSPs except EMIs 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.

EMIs should download the payment services complaints form available here, complete it electronically in Excel, and send it to us by email to regulatory.reports@fca.org.uk.

Report required – REP017 Payments Fraud Report

Required to submit: All PSPs (credit institutions, PIs, EMIs, RAISPs)

Frequency: ~~Annual~~SPIs, SEMIs and RAISPs report annually, all other PSPs report twice yearly.

Submission date: Within ~~1 month~~2 months of the reporting end date (the reporting period runs from 1 January – 30 June and from 1 July - 31 December)

Method of submission: Gabriel (~~Email~~email if EMI or SEMI)

Handbook references: SUP 16.13 (Reporting under the Payment Services Regulations), SUP 16 Annex ~~27E~~ 27ED (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. PSPs are required to make every effort to comply with the EBA Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2)[51] which specify the data to be reported to the FCA. We have implemented these Guidelines in the form of the 'REP017 Payments Fraud Report'. All PSPs should complete this form in order to comply with the EBA Guidelines.

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

All PSPs except EMIs 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.

EMIs should download the REP017 Payments Fraud Report ~~available.~~ (available here~~.~~) complete it electronically in Excel, and send it to us by email to regulatory.reports@fca.org.uk.

~~Reports required – Operational and Security Risk Report (REP018) – PSD2~~

52 The EBA Guidelines on fraud reporting are available here: https://www.eba.europa.eu/documents/10180/2281937/Guidelines+on+fraud+reporting+under+Article+96%286%29%20PSD2+%28EBA-GL-2018-05%29.pdf

Required to submit: All PSPs (credit institutions, PIs, EMIs when offering payment services, and RAISPs).

Frequency: PSPs must report to us at least once per calendar year. PSPs may report up to once per quarter, but no more frequently. If PSPs choose not to submit a report in a particular quarter they should access the form and answer "No" to question 1. Where a PSP submits less than four reports per year, a "nil return" for the quarters during which a PSP is not reporting can be submitted at the same time as the completed report is submitted.

Method of submission: Gabriel, except EMIs (please see "Process", below)

Handbook references: SUP 16.13.9 to 16.13.17 and SUP 16.13.18 to 16.13.21 and SUP16 Annex 27H

Content and purpose

This notification is required under Regulation 98 of the PSRs 2017. Each payment service provider must provide us with an updated and comprehensive assessment of the operational and security risks relating to the payment services it provides and on the adequacy of the mitigation measures and control mechanisms implemented in response to those risks.

Requiring PSPs to submit this report helps us discharge our supervisory functions effectively. This report will strengthen our understanding of the operational and security risks encountered by PSPs in the payment services they offer and whether PSPs have appropriate systems and controls in place to address operational and security risks.

The operational and security risk report should include the results of the latest assessment of the operational and security risks related to the payment services provided by the PSP and an assessment of the adequacy of the mitigation measures and control mechanisms implemented in response to those risks. REP018 contains further details of what the risk assessment and assessment of the adequacy of mitigation measures should include.

We also use the information submitted in this report to assess whether PSPs relying on the SCA-RTS Article 17 exemption ("corporate payment exemption") from strong customer authentication have in place processes and protocols that guarantee at least equivalent levels of security to those provided for by PSD2 (see SUP 16.13.18). PSPs relying on this exemption must submit the required information in this report at least 3 months in advance of the date of intended use of the exemption.

Process

Operational and Security Risk Report (REP018) – PSD2 is available at SUP 16 Annex 27G.

All PSPs except EMIs 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 (it is the firm's responsibility to comply with their reporting requirements. The schedule is for indicative purposes only).

EMIs should download the REP018 Operational and Security Risk Report, complete it electronically in Excel, and email it to ~~t to~~ regulatory.reports@fca.org.uk. We would not expect EMIs to submit a 'nil return' to us.

Report required – REP020 Statistics on the availability and performance of a dedicated interface

Required to submit: ASPSPs that opt to provide a dedicated interface under SCA-RTS Article 31

Frequency: Quarterly

Submission date: Within 1 month of every publication on the ASPSP's website of the statistics required to be published under SCA-RTS Article 32(4)

Although the SCA-RTS does not give details of what quarterly means in terms of publication of the statistics, we would expect publication to be aligned to standard calendar quarters. This means the first publication would be a partial quarter in respect of 14 September to 30 September, and publication would align with each full quarter thereafter.

Method of submission: Gabriel (email if EMI or SEMI)

Handbook references: SUP 16.13.22 to 16.13.24 and SUP16 Annex 46AD

Content and purpose

In this report, the ASPSP is asked to provide the same statistics that it has published on its website under SCA-RTS Article 32(4). The published and reported statistics should meet the requirements of the EBA Guidelines on the conditions to be met to benefit from an exemption from the contingency mechanism under SCA-RTS Article 33(6). This includes key performance indicators on the availability and performance of the dedicated interface in accordance with EBA Guideline 2.

The purpose of this report is to ensure that we receive information relevant to our ongoing assessment of whether an ASPSP continues to meet the conditions for exemption from the contingency mechanism, under SCA-RTS Article 33(6) and more generally to understand the availability and performance of ASPSPs' dedicated interfaces.

Process

ASPSPs except EMIs should follow the instructions on the Gabriel online system to submit REP020 electronically. Gabriel can also be used to view a tailored schedule of your reporting requirements.

ASPSPs that are EMIs should send REP020, (available here) to us by email to regulatory.reports@fca.org.uk.

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 authorised EMI or authorised PI's accounting reference date.

Method of submission: Gabriel (email if EMI)

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 regulation 37 of the 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

All PSPs except EMIs should follow the instructions on the Gabriel online system to submit the return REP002 electronically. More information about annual controllers reporting can be found at: https://~~www.fca.org.uk/firms/~~ www.fca.org.uk/firms/regulatory-reporting/annual-controllers-reporting

EMIs should download REP002 availab~~le~~ e here, complete it electronically in Excel, and send it to us by email ~~to~~ to regulatory.reports@fca.org.uk.

All PSPs except EMIs should follow the instructions on the Gabriel online system to submit the return REP001 electronically. More information about close links reporting can be found at: https://www.fca.org.uk/firms/regulatory-reporting/close-links

EMIs should download REP001 availab~~le~~ e here complete it electronically in Excel, and send it to us by email ~~to~~ to regulatory.reports@fca.org.uk.

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: Online survey

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 we receive 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

Electronic money institutions are not currently reporting through Gabriel, our regulatory reporting system. We have therefore made alternative arrangements for completion of the return via an ~~n~~online ~~survey~~survey.

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. More information can be found on our website: https://www.fca.org.uk/firms/electronic-money-reporting-requirements

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 us in respect of the 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.

13.8 If the accounts are audited and filed with Companies House they should be sent to us at the same time. If, as small firms, they are not required to file audited accounts with Companies House we expect the 'payment services business only' accounts to be sent to us within nine months of the PI or EMI's Accounting Reference Date (ARD).

13.9 Information required under regulation 24 of the PSRs 2017 and regulation 25 of the EMRs should be provided in electronic form (scanned if necessary) by email to regulatory.reports@fca.org.uk.

Late submission of returns

13.10 All 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.

Part II: Notifications

13.11 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 in line with SUP 15.14.6 D
Method of submission: Connect
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) of the PSRs 2017, a credit institution that refuses a PSP's request to access payment account services must provide duly motivated reasons for the refusal to us. We will use the information provided in this notification for the purposes of supervising compliance with regulation 105 of the PSRs 2017 (jointly with the PSR). Please refer to **Chapter 16 – Payment service providers' access to payment account services** for more information.
Process
Credit institutions should follow the instructions on the Connect online system to submit their notification electronically.

Notification required – NOT003 AIS/PIS denial
Required to notify: account servicing payment service providers (ASPSPs)
When to notify: The ASPSP must notify us immediately in line with SUP 15.14.12 D
Method of submission: Connect
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) of the PSRs 2017, an ASPSP that denies a PISP or AISP access to payment service users' payment accounts must submit a notification to us. 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
ASPSPs should follow the instructions on the Connect online system to submit their notification electronically.

Notification required – NOT004 Notification that a fraud rate has been exceeded (SCA-RTS Article 20)

Required to notify: PSPs making use of the transactional risk analysis exemption

When to notify: A PSP must submit the notification in line with SUP 15.14.34

Method of submission: Connect

Handbook reference: SUP 15.14.29 to 15.14.37 (Notification that a fraud rate has been exceeded (SCA-RTS Article 20)), SUP 15 Annex 12 (Form NOT004)

Content and purpose

Article 18 of the SCA-RTS permits PSPs not to apply strong customer authentication where the payer initiates a remote electronic payment transaction identified by the PSP as posing a low level of risk according to the transaction monitoring mechanism referred to in Article 2 and where certain other conditions set out in Article 18 of the SCA-RTS are met. One of these conditions requires that the fraud rate for that type of transaction and amount, calculated in accordance with Article 19 of the SCA-RTS, is equivalent to or lower than the reference fraud rate indicated in the Annex to the SCA-RTS. Where a PSP's monitored fraud rate exceeds the applicable reference fraud rate, Article 20(1) of the SCA-RTS requires it to immediately report to the FCA, providing a description of the measures that it intends to adopt to restore compliance with the reference fraud rates.

See also, **Chapter 20 – Authentication** for more information.

Process

PSPs should follow the instructions on the Connect online system to submit their notification electronically.

Notification required – NOT005 Problems with a dedicated interface (SCA-RTS Article 33(3))

Required to notify: ASPSPs, AISPs, PISPs and CBPIIs

When to notify: The ASPSP, AISP, PISP or CBPII must notify us without undue delay in line with SUP 15.14.38

Method of submission: Connect

Handbook reference: SUP 15.14.38 (Notifying problems with a dedicated interface (Article 33(3) of the SCA-RTS)), SUP 15 Annex 9 (Form NOT005 in SUP 16 Annex 13)

Content and purpose

Under SCA-RTS Article 33(3), ASPSPs, AISPs, PISPs and CBPIIs are required to report problems with dedicated interfaces without undue delay. Please refer to **Chapter 17 – Payment initiation and account information services and confirmation of availability of funds** for more information.

Process

ASPSPs, and PSPs carrying out AIS, PIS and CBPII, should follow the instructions on the Connect online system to submit their notification electronically.

Notification required – Credit institutions providing (or intending to provide) account ~~information or~~ 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 15 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 of the PSRs 2017 (activities involving limited network payment instruments which do not constitute payment services), where the total value of the payment transactions executed through such services in any period of 12 months exceeds €1million.

When to notify: Service providers must notify as directed here:

https://www.fca.org.uk/firms/limited-network-exclusion

Method of submission: Connect

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.

For more information on the scope of the limited network exemption please see PERG 15 Q.40.

Process

Businesses should follow the instructions on Connect to submit their notification electronically.

More details are available on our website: https://www.fca.org.uk/firms/limited-network-exclusion

Notification required – Regulation 39 Notification of services carried out under the electronic communications exclusion

Required to notify: A provider (or proposed provider) of services for payment transactions falling within paragraph 2(l) of Schedule 1 of the PSRs 2017 (activities involving electronic communications networks or services which do not constitute payment services) and Regulation 3B(b) of the EMRs (as amended by paragraph 5(3B) of Schedule 8 to the PSRs 2017).

When to notify: Service provides must notify as directed here: https://www.fca.org.uk/firms/electronic-communications-exclusion

A service provider is also required to provide an audit opinion. The timing of the audit opinion depends on the service providers' accounting reference date. See direction for more details.

Method of submission: Connect

Content and purpose

This notification is required under regulation 39 of the PSRs 2017 and regulation 3B of the EMRs. A person who provides or intends to provide a service falling within the electronic communications exclusion must submit to us: (a) a notification including a description of that service (PSRs 2017) or a description of the transactions for which the monetary value is intended to be used (EMRs); and (b) an annual audit opinion testifying that the transactions for which the services is provided comply with the applicable financial limits.

For more information on the scope of the electronic communications exclusion please see PERG 15-Q41A.

Process

Businesses should follow the instructions on Connect to submit their notification and auditor's report electronically. ~~More details are available on our website: https://www.fca.org.uk/firms/electronic-communications-exclusion~~

More details are available on our website: https://www.fca.org.uk/firms/electronic-communications-exclusion

Notification required – Notification of major operational or security incidents – PSD2

Required to notify: All PSPs are required to notify us without undue delay if they become aware of a major operational or security incident. SUP 15.14.20 D requires PSPs to comply with the EBA Guidelines on major incident reporting under PSD2. These Guidelines specify the criteria a PSP should use to assess whether an operational or security incident is major and needs to be reported to us. These Guidelines also specify the format for the notification and the procedures the PSP should follow. PSPs are required to submit an initial, intermediate and final notification.

When to notify: The notification channel is usually available at all times.

The **initial notification** should be submitted to us within the first four hours from the moment the incident was detected, or, if the notification channel is not available or operational at that time, as soon as it becomes available or operational again.

We may direct PSPs to submit initial notifications at times other than those specified above.

An **intermediate report** should be submitted, using the same method, every time there is a relevant status update to the incident. As a minimum it should be submitted by the date indicated in the previous report (either the initial report or the previous intermediate report).

A **final report** must be submitted when the root cause analysis has taken place (regardless of whether mitigation measures have already been implemented or the final root-cause has been identified) and there are actual figures available to replace any earlier estimates.

Method of submission: Connect

Handbook references: SUP 15.14.16 to 15.14.22 and SUP 15 Annex 11D

Content and purpose

This notification is required under Regulation 99 of the PSRs 2017. The notification must include the information set out in the template form cited in SUP 15 Annex 11D and must be in writing.

Requiring PSPs to notify us of major operational or security incidents helps us discharge our supervisory functions by providing us with information on the most serious operational and security incidents.

Process

Businesses should follow the instructions on Connect to submit their notifications electronically

~~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:~~

~~Reporting to host member states from PIs having agents or branches within host member state territories as may be required under article 29(2) of PSD2. This is dependent on EBA RTS to be developed under article 29(6) of PSD2.~~

~~Reporting required in accordance with the RTS developed under article 98 of PSD2. 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.~~

14 Enforcement

14.1 This chapter describes our enforcement approach. It is relevant to payment service providers (PSPs) and e-money institutions (EMIs) and persons who are subject to our enforcement action under the Payment Services Regulations 2017 (PSRs 2017) or the Electronic Money Regulations 2011 (EMRs).[~~45~~53]

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).[~~46~~54] It 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 follows our approach set out in EG 2.4 and covers provision of payment services by persons that are not PSPs or issuance of e-money by persons that are not EMIs.

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 our 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

[~~45~~53] 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.

[~~46~~54] Any breaches of DISP will be enforced using the normal FSMA procedures.

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?
- 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 breach(es)?
- 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 EMI 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 EMIs, agents and excluded providers to provide restitution to their customers.

14.10 We can cancel, vary or place requirements on a PI, RAISP 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, or failure to meet the minimum standards to remain authorised or registered, 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 EMIs and other persons who breach our rules or the requirements of the PSRs 2017 and EMRs can be found in Chapter 19 of 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 European Economic Area (EEA) authorised payment institutions (PIs), EEA authorised EMIs and EEA registered authorised account information service providers (RAISPs). We can take precautionary measures pending action by the home state competent authority (i.e. the competent authority where the authorised PI, authorised EMI or RAISP is authorised or registered). We may take immediate action where it is necessary to address a serious risk to the collective interest of customers in the UK. We will withdraw such 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.[~~47~~55]

Where can I find more information?

14.22 EG 19 sets out more detail on the use of our non-FSMA enforcement powers (e.g. in relation to the PSRs 2017, and the EMRs and the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017). 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.

~~47~~55 Third party rights also apply to proposed action to cancel an authorisation or registration, to take disciplinary measures or to require restitution.

15 Fees

Introduction

15.1 All payment service providers (PSPs), including providers of account information services (AIS) and payment initiation services (PIS), and e-money issuers are subject to fees that we are able to levy to recover the costs of meeting our regulatory responsibilities under the Payment Services Regulations 2017 (PSRs 2017) and Electronic Money Regulations 2011 (EMRs). This chapter covers fees payable specifically by payment institutions (PIs) and e-money institutions (EMIs) and fees applicable to PSPs and e-money issuers which we collect on behalf of the Financial Ombudsman Service.

15.2 Since we receive no subsidies from other sources but are funded entirely by the firms we regulate, our fees are intended to recover our costs in a way that is as fair and efficient as possible. To target the recovery of our regulatory costs, we group fee-payers into 'fee-blocks.' These enable us to link together firms with similar permissions and allocate our costs to them. We then recover our costs through periodic fees (variable annual fees), based on a metric known as a 'tariff base'.

15.3 We consult on regulatory fees and levies each year. In the autumn, we publish policy proposals for regulatory fees and levies. This is followed in spring with a consultation paper (CP) on the periodic fee rates to be charged for the following year. These are finalised in a Policy Statement (PS), which we issue in June or July. Firms are invoiced from July. All of these publications are likely to contain proposals affecting PSPs and e-money issuers, who should look out for them on our website so they can send us their comments.

Fees: PIs, EMIs and RAISPs

15.4 PIs and EMIs fall into the 'G' fee-block. The fees of authorised PIs, authorised EMIs and registered account information service providers (RAISPs) are based on income. Small PIs and small EMIs pay a flat fee.

15.5 See the Fees Manual (FEES) of the Handbook for further information on fees:

- Information on **application fees** is contained in FEES 3 Annex 8 and in FEES 3 Annex 10 for PIs and EMIs, respectively; and
- FEES 4 Annex 11R provides information on **periodic fees**.

15.6 In addition, more information is available on the following web pages:

- Fees and levies: https://www.fca.org.uk/firms/fees
- How we decide rates for annual fees: https://www.fca.org.uk/firms/fees/how-we-decide-rates-annual-fees
- Fees publications: https://www.fca.org.uk/firms/fees/publications
- Fees calculator: https://www.fca.org.uk/firms/calculate-your-annual-fee/fee-calculator
- FCA fees manual: https://www.handbook.fca.org.uk/handbook/FEES.pdf

Payment services fees proposal for the Financial Ombudsman Service

15.7 PSPs and e-money issuers are subject to the jurisdiction of the Financial Ombudsman Service. The Financial Ombudsman Service charges an annual levy to firms in its compulsory jurisdiction, which we collect on its behalf. A case fee is payable for every chargeable case, but is collected by the Financial Ombudsman Service once it has closed a chargeable case.

15.8 PSPs and e-money issuers already subject to the Financial Ombudsman Service will continue to contribute to the general levy through their existing industry fee blocks.

16 Payment service providers' 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 Payment Services Regulations 2017 (PSRs 2017). In this chapter, unless stated otherwise, references to 'we' or 'us' mean the FCA and the Payment Systems Regulator together. This chapter also appears as chapter 3 of the Payment Systems Regulator's Approach Document.[~~48~~56]

16.2 This chapter sets out our guidance on how we will apply the provisions of regulation 105 of the PSRs 2017, which deals with PSPs' access to payment account services. It is relevant to credit institutions and to PSPs and prospective PSPs who wish to access these services in order to provide their own payment services. For the purposes of regulation 105 of the PSRs 2017 and this chapter, "PSPs" means:

- authorised PIs
- small PIs
- RAISPs
- EEA authorised PIs
- EEA RAISPs
- EMIs

16.3 Regulation 105 of the PSRs 2017 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 European Economic Area (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) of the PSRs 2017 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.

[~~48~~56] https://www.psr.org.uk

The requirements of regulation 105

16.6 Regulation 105 of the PSRs 2017 requires that credit institutions must grant PSPs access to payment account services on a proportionate, objective and non-discriminatory (POND) basis. The regulation also requires credit institutions to:

- provide PSPs that enquire about access to payment account services with the criteria that 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

16.8 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 payment institution is still a commercial one, with credit institutions able to take into account cost and risk."

16.9 We agree with this statement. In our view, the effect of regulation 105 of the PSRs 2017 is to ensure that credit institutions should consider applications from PSPs individually and on their own merits. They should not have policies based on restricting access to those services for certain categories or types of PSPs, without considering the specific risks posed by the business and ways in which an individual PSP might mitigate the risks.

16.10 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 of the PSRs 2017 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.

16.11 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):

- Does the credit institution offer the payment account service that the PSP or prospective PSP has requested? How much cost and risk would it need to incur in

order to do so?

- 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 paragraph 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 (e.g. by charging a higher price or requiring additional reporting as opposed to restricting access entirely)?

16.12 Factors relating to the process by which the decision was reached will also be relevant to our assessment, e.g:

- 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

16.13 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 of the PSRs 2017 requires credit institutions to provide these criteria in response to access enquiries from potential applicants.

16.14 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 (e.g. 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.

16.15 Where enquiries are made, credit institutions should provide their criteria to the potential applicant in written form, or, where it is made publicly available, e.g. on a website, direct the enquiring party to the relevant information.

16.16 The information that 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. This does not, however, extend to disclosing commercially sensitive information about the credit institution's business strategies or risk appetites.

16.17 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.

16.18 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 on whether or not to provide payment account services.

16.19 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

16.20 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.

16.21 Such arrangements might cover, for example, how clear accountability for decisions is achieved, how relevant staff are trained and how compliance is monitored internally. It will be up to each credit institution, however, to be able to demonstrate that it is maintaining appropriate arrangements.

16.22 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

16.23 Regulation 105 of the PSRs 2017 requires that access to payment account services is sufficiently extensive to allow the PSP to provide payment services in an unhindered and efficient manner.

16.24 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 (e.g. 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 of the PSRs 2017 and this chapter.

16.25 Regulation 105 of the PSRs 2017 does not require credit institutions to provide types of products and services that they do not already provide. We would, however, 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.

16.26 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) of the PSRs 2017 and the following section.

Notifying the FCA where access is refused or withdrawn

16.27 Regulation 105(3) of the PSRs 2017 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. This includes refusals where the reason for refusal is because the credit institution does not provide the payment account service requested. Under regulation 105(3) of the PSRs 2017, the FCA will share notifications with the Payment Systems Regulator. There is no requirement under regulation 105 of the PSRs 2017 for credit institutions to provide the duly motivated reasons to the PSP or prospective PSP. We expect that in practice, credit institutions will tell the PSP or prospective PSPs their decision except to the extent it is unlawful to do so (e.g. due to restrictions on 'tipping off'- see guidance at paragraph 19.20 in **Chapter 19 - Financial crime**).

Refusal and withdrawal

16.28 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.

16.29 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. However, a notification is not required if a potential applicant has enquired and has the opportunity to apply, but decides of its own volition not to apply.

16.30 Similarly, a refusal to grant access following consideration of an application should be notified to the FCA with duly motivated reasons.

16.31 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

16.32 Regulation 105(3) of the PSRs 2017 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. Credit institutions are not required to provide separate or duplicate notification to the Payment Systems Regulator.

16.33 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) of the PSRs 2017.

16.34 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.

16.35 Where a credit institution intends to withdraw access from all customers of a particular payment account service, for example, if it intends to discontinue a particular product, or withdraw from providing services altogether, we would expect it to contact the FCA to discuss this rather than submitting a notification to the FCA for each PSP under SUP 15.14.3. The FCA will advise whether and in what form duly motivated reasons are to be provided.

Providing duly motivated reasons to the FCA

16.36 In the event of a refusal or withdrawal, a credit institution must submit the notification form **NOT002 Payment Account Service rejections or withdrawals**, completed in accordance with the notification rule SUP 15.14.3D.

16.37 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

16.38 The FCA and Payment Systems Regulator must each maintain arrangements designed to enable payment service users and other interested parties (such as PSPs) to submit complaints to them about alleged infringements of the PSRs 2017 (see **Chapter 11 – Complaints Handling**). This includes complaints where a requirement imposed by or under regulation 105 of the PSRs 2017 might have been breached by a credit institution. We will consider complaints from individuals that allege infringements of regulation 105 of the PSRs 2017, together with, and in light of, information we receive in notifications under regulation 105(3) of the PSRs 2017.

16.39 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.

16.40 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 PSRs 2017 powers and procedures guidance, which can be found at Appendix 1 of its Approach Document.

17 Payment initiation and account information services and confirmation of availability of funds

~~**Note: This chapter references Regulatory Technical Standards and Guidelines yet to be finalised at time of publication. It will be updated once the final documents are published in the Official Journal of the European Union or, in the case of Guidelines, by the EBA.**~~

Introduction

17.1 Account information services (AIS) and payment initiation services (PIS) ~~– two services not previously regulated by us –~~ are now in the scope of the Payment Services Regulations 2017 (PSRs 2017). **Chapter 2 – Scope** and ~~PERG 15.~~ 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 (PSP) providing and maintaining the payment account for the payer is referred to in the PSRs 2017 as the 'account servicing payment service provider' (ASPSP~~).~~) provided the account is accessible online. ASPSPs include businesses that provide 'payment accounts' such as banks, building societies, payment institutions (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). The terms 'AISP' and 'PISP' in this guidance refer to providers of AIS and PIS who are authorised or registered (as relevant) ~~by us~~ to provide those services or are otherwise PSPs providing those services under the PSRs 2017. Any PSP 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 the Financial Services and Markets Act 2000 (FSMA). For example, if a credit institution provides PIS or AIS, they will be ~~a~~covered by the terms PISP or AISP in relation to ~~the~~their provision of that service.

17.4 The PSRs 2017 also create a framework enabling a PSP that has issued a card-based payment instrument to a payer to obtain confirmation from an ASPSP which holds an account for that payer whether the amount necessary for a payment transaction is available on that account, thereby allowing the card-based payment instrument issuer to better manage and reduce its credit risk. The institution issuing the card-based payment instrument 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~~CBPIIs are the Regulatory Technical Standards on strong customer authentication and common 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.[49][57] The security measures referred

49 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

to in regulations 68(3)(c), 69(2)(a) and), 69(3)(d), 70(2)(a) and), 70(3)(c), 77(4)(c) and), 77(6) and 100 of the PSRs 2017 (secure communication and authentication) and the associated SCA-RTS will apply to firms from 18 months after the 14 September 2019. The European Banking Authority (EBA) issued an Opinion on the implementation of the SCA-RTS (the 'EBA Opinion'),[58] which provides clarity on certain requirements. The SCA-RTS enters into force. The SCA-RTS, once it becomes a Commission Delegated Regulation, and the EBA Opinion should be read alongside the relevant sections in this chapter. Guidance on the SCA-RTS

57 The Commission Delegated Regulation (EU) 2018/389 (the SCA-RTS) is available here https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN

58 https://www.eba.europa.eu/documents/10180/2137845/Opinion+on+the+implementation+of+the+RTS+on+SCA+and+CSC+%28EBA-2018-Op-04%29.pdf

requirements concerning strong customer authentication is given in **Chapter 20 – Authentication**.

17.6 Having effective control mechanisms in place to manage operational and security risks is a key element of the regime created by PSD2. For example, the information that we assess as part of an application for authorisation or registration to provide AIS or authorisation to provide PIS includes a statement of the applicant's security policy~~, covering~~. This covers a description of the applicant's security control and mitigation measures, which are intended to provide adequate protection to users, and how these measures ensure a high level of technical security and data protection, including in relation to IT systems used by the applicant. Regulation 98 of the PSRs 2017 explicitly requires a PSP 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, once authorised or registered. **Chapter 18 – Operational and security risks** contains further information.

17.7 Where an AISP or a PISP outsources any operational function relating to its provision of AIS or PIS, the AISP or PISP needs to ensure that it has arrangements that allow it to fulfil the conditions of registration or authorisation, and will need to provide us with this information to demonstrate this when applying, as we set out in **Chapter 3 – Authorisation and Registration**. Changes in outsourcing arrangements must be notified to us as detailed in **Chapter 4 – Changes in circumstances of authorisation and registration**.

17.8 Many other requirements applicable to PISPs and AISPs are set out in **Chapter 8 – Conduct of business requirements**. 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.

17.9 For AISPs, which conduct of business requirements apply will depend on whether they are providing any payment services other than AIS. A business offering AIS and no other payment service can apply to us to become a registered account information service provider (RAISP) instead of seeking full authorisation. RAISPs are subject to a more limited number of conduct of business requirements than other PSPs. Otherwise, AISPs that are not subject to reduced requirements must follow all of the conduct of business requirements to the extent that they are applicable to the AISP's business model and the way that the AISP interacts with its customers.

17.10 This chapter outlines and provides guidance in relation to the requirements introduced in the PSRs 2017 that relate to AIS and PIS. This chapter is split into ~~seven~~thirteen parts:

- scope of accounts subject to the requirements
- requirements on ASPSPs
- requirements on PISPs, AISPs and CBPIIs
- ~~requirements on ASPSPs, PISPs, AISPs and CBPIIs when communicating and interacting with their customers in relation to these services~~
- other requirements applicable to PISPs

- other requirements applicable to AISPs
- requirements on ASPSPs, CBPIIs, PISPs and AISPs when communicating and interacting with their customers in relation to these services

- transitional arrangements before the SCA-RTS becomes applicable
- requirements on all ASPSPs for secure communication
- requirements on ASPSPs providing access via a dedicated interface
- exemption from the contingency mechanism
- exemption criteria and FCA information requirements
- revoking exemptions
- reporting problems with the dedicated interface

Scope of accounts subject to the requirements

17.11 PERG 15 provides further guidance on the activities that constitute AIS and PIS.

17.12 Regulations 68, 69 and 70 of the PSRs 2017 only apply to 'payment accounts' which are 'accessible online'.

17.13 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 15.3. Under this guidance, a payment account can include, but is not limited to, current accounts, e-money accounts, flexible savings accounts, credit card accounts and current account-mortgages.

17.14 The meaning of 'accessible online' is not defined under the PSRs 2017. 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. Whether an account is accessible online should not be dependent on whether a particular customer has chosen to activate online banking services with the ASPSP. As a result, an ASPSP should not deny an AISP or PISP access to a customer's account or refuse to give confirmation of availability of funds to a CBPII on the basis that the customer has not registered for online banking. The customer may, however, need to activate online banking 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.

17.15 The purposes for which the specific account can be accessed online also needs to be considered when determining whether an account is 'accessible online'. Whether regulations 68, 69 and 70 of the PSRs 2017 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.

17.16 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))

17.17 When an ASPSP's customer uses an AIS or gives explicit consent for a payment to be made through a PIS in accordance with regulation 67 of the PSRs 2017, the ASPSP must comply with certain obligations. This consent can be provided directly to the ASPSP or provided via a PISP (e.g. where the PISP transmits the personalised security credentials) or via the payee.

17.18 As per regulation 68(55)(b) of the PSRs 2017, 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.

17.19 Guidance is given at paragraph 17.~~44~~53 on the meaning of 'explicit consent'.

Communication with CBPIIs, PISPs and AISPs (regulations 68(3)(c) 69(2)(a) and 70(2)(a))

17.20 Regulations 68(3)(c) 69(2)(a) and 70(2)(a) of the PSRs 2017 apply ~~18 months after the~~from 14 September ~~SCA-RTS is published in the Official Journal of the European Union.~~2019. At this point, an ASPSP must communicate with CBPIIs, PISPs and AISPs (including with their agents or outsourcers where providing relevant aspects of their service) in accordance with the SCA-RTS (in particular SCA-RTS Articles 30 to 36). In summary, the SCA-RTS will require ASPSPs to communicate securely and to ~~to~~ offer a method of access to AISPs, PISPs and CBPIIs which complies with a number of minimum standards, including requirements for identification, traceability of transactions (in line with SCA-RTS Article 29), the security of communication sessions and data exchange. Where an ASPSP provides multiple secure methods of access, at least one of those methods of ~~access~~ access[59] must meet all of the ASPSP's obligations under the PSRs 2017 (including the SCA-RTS ~~when it becomes applicable~~).

17.21 Further guidance on ASPSPs' obligations before the SCA-RTS applies can be found in paragraphs 17.~~66~~80-17.~~71~~85.

Confirmation of the availability of funds (regulation 68(4)) – CBPII

17.22 If the ASPSP receives a request that meets the requirements of regulation 68(2) of ~~the~~ the PSRs 2017, and in accordance with SCA-RTS Article 36(1)(c), the ASPSP must immediately provide a ~~yes~~'yes' or ~~no~~ '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, and therefore this is likely to mean the answer must be provided as soon as the request is received.

17.23 In line with the EBA Opinion, when determining whether to give a 'yes' or 'no' response to the request for confirmation of the availability of funds from a card-based payment

59 Whether access is via a dedicated interface or by allowing PISPs, AISPs, CBPIIs to use the interface used for authentication and communication with the ASPSP's payment service users.

instrument issuer, the ASPSP is required to take into account, at the time the request is received, the same information it would consider if the customer was executing a payment transaction directly with the ASPSP. Such information may include, for example, the available balance, any agreed overdraft and any incoming or outgoing payments that will affect the funds available.

Confirmation of the availability of funds – PISP

17.24 The EBA Opinion clarifies that Article 36(1)(c) applies to PSPs, rather than solely CBPIIs. This means the requirement for ASPSPs to provide the 'yes' or 'no' confirmation of the availability of funds response also applies to requests received from PISPs. The EBA notes that the 'yes' or 'no' confirmation will help PISPs to manage the risk of non-execution. PISPs should only make a request for the 'yes' or 'no' confirmation, when they intend to initiate a payment.

17.25 When determining its response to a PISP's 'yes' or 'no' request, the ASPSP should take into account, at the time the request is received, the same information (e.g. available balance, agreed overdraft, incoming and outgoing funds) it would consider if the customer was executing a payment transaction directly with the ASPSP. The ASPSP should provide a 'yes' response if it would, in the circumstances, execute a payment instruction given by a customer directly.

17.26 The EBA Opinion also sets out that where an ASPSP does not have a system that enables it to adequately respond to the confirmation request sent by a PISP, it should be possible for a PISP to request information related to the availability of sufficient funds. The ASPSP should provide or make available to the PISP the same information the ASPSP would use itself to determine the 'yes' or 'no' response.

17.27 Where a PISP intends to make such a request, we expect the PISP to obtain the payer's explicit consent in advance, in line with regulation 97 of the PSRs 2017 rather than on a transaction-by-transaction basis. In our view, there is no requirement for the PISP to have additional authorisation or registration as an AISP for this purpose or for the ASPSP to check that the PISP has obtained the customer's explicit consent.

Information on the initiation of the payment transaction (regulation 69(2)(b))

17.~~23~~28 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.~~24~~29 In our view, the requirement to provide or make available 'all information on the initiation of the payment transaction and all information accessible to the ASPSP regarding the execution of the payment transaction' would include, as a minimum, the information, as specified in regulation 45 of the PSRs 2017, that would be provided or made available to the customer directly if the customer initiated a payment. ~~Information regarding the 'execution of the payment transaction'~~It would therefore include ~~information regarding a failure or refusal to execute a transaction.~~;

- a reference enabling the payer to identify the payment transaction and, where appropriate, information relating to the payee
- the amount of the payment transaction in the currency used in the payment order

- the amount of any charges for the payment transaction payable by the payer (to the payer's PSP) and, where applicable, a breakdown of the amounts of such charges

- where an exchange rate is used in the payment transaction (by the payer's PSP) and the actual rate used in the payment transaction differs from the rate provided in accordance with regulation 43(2)(d) of the PSRs 2017, the actual rate used or a reference to it, and the amount of the payment transaction after that currency conversion

- the date on which the PSP received the payment order

17.30 Additionally, under regulation 44 of the PSRs 2017, a PISP is required to provide the payer certain additional information after the initiation of the payment order. This includes confirmation of the successful initiation of the payment order with the payer's ASPSP. It is necessary, therefore, for the ASPSP to provide this confirmation to the PISP, in order for the PISP to provide it to the payer. The ASPSP must also provide any other information on the initiation and execution of the payment transaction that it would otherwise provide directly to the payment service user pursuant to SCA-RTS Article 36(2).

Treatment of data requests and payment orders (regulations 69(2)(c) and 70(2)(b))

17.~~25~~31 Though they may provide factual information explaining AIS and PIS, 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.~~26~~32 An ASPSP must treat data requests and payment orders from AISPs and PISPs the same as those that come directly from its customers unless it has objective reasons to treat them differently. In our view, the references to "objective reasons" in regulations 69(2)(c) and 70(2)(b) of the PSRs 2017 would generally have the same meaning as in ~~Article~~regulation 71(7) of the PSRs 2017, as objective and duly evidenced reasons relating to fraudulent or unauthorised access by that AISP or PISP can potentially justify differential treatment.

AIS data requests

17.~~27~~33 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, provided this does not include sensitive payment data (see section 17.63 on sensitive payments data below). The amount of information which is required to be ~~disclosed~~ made available will, therefore, differ across ASPSPs and across accounts. In line with the EBA Opinion, ASPSPs should make available the maximum amount of information that would be available to the customer across the channels the customer uses to access their payment account directly. For example, if there are more data available to the customer directly through the web browser channel than the mobile app, it is the amount of data available through the web browser that should be made available via the AISP. To give some examples, we would expect the following sorts of information to be ~~included where the information is~~made available ~~to the customer directly~~via an AISP:

- information relating to the account, ~~such as~~ including the name ~~on~~(s) of the

account holder(s)
and the account number; ~~and~~combined with

- 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. In our view this does not, however, 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.~~28~~34 Aside from the above, in line with the EBA Opinion, the information ASPSPs are required to provide or make available to a PISP or an AISP does not include information concerning the identity of the customer (for example, address, date of birth or national insurance number) as such information is not specifically required for the provision of PIS or AIS. However, the PSRs 2017 do not prohibit PISPs or AISPs and ASPSPs from agreeing to share such information (as long as data protection legislation is complied with).

17.35 PERG Q25A provides guidance on what the consolidated information provided to the customer must include for the service to require regulation as an account information service.

PIS payment orders

17.36 For PIS, 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.~~ directly.

17.~~29~~37 In order to meet this requirement, and in line with the EBA Opinion, we expect ASPSPs to allow each customer to initiate a payment via a PISP to the same level of functionality that is available to a customer if they initiate a payment directly with their ASPSP. If the customer is able to initiate, for example, international payments, recurring transactions or a batch file of payments online, they should also be able to do so via a PISP, irrespective of the channel the customer has used to access the PISP. 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.~~ An ASPSP does not need to allow customers access via a PISP to any online functionality other than initiating payments (e.g. ordering a cheque book or cancelling a direct debit).

17.~~30~~38 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.~~31~~39 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 customer 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~~/~~s or 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; and

- 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.~~32~~40 An ASPSP is prohibited from requiring a PISP or an AISP to enter into a contract with it before complying with its obligations under regulations 69 and 70 of the PSRs 2017 and under the SCA-RTS. In our view, this means that access should not depend on the AISP or PISP agreeing to any specific arrangements with the ASPSP (e.g. payment or liability arrangements). Similarly, ASPSPs requiring or suggesting to AISPs or PISPs that a contractual arrangement is required would not be permitted.

17.~~33~~41 In our view, this does not, however, prohibit the parties from putting contractual arrangements, or arrangements to address liability between them, 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 2017 and the SCA-RTS (e.g. 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~~ regulations 71(7~~),~~) and 71(8))

17.~~34~~42 The regulations and this guidance do not apply to ASPSPs' decisions in relation to payment orders or access requests to payment account data from businesses that are not authorised or registered providers of AIS or PIS, and are not otherwise PSPs under the PSRs 2017. See paragraphs 2.23 – 2.24 of **Chapter 2 – Scope** and 3.9 of **Chapter 3 – Authorisation and registration** for further details on our Register and its role in establishing which businesses are authorised or registered.

17.~~35~~43 An ASPSP may 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. This does not diminish an ASPSP's ability to refuse payment orders or information requests made through AISPs or PISPs for legitimate reasons which would have led them to refuse those orders or requests from the customer themselves (in line with regulation 69(2)(c) and regulation 70(2)(b) of the PSRs 2017; see also regulation 82(5) of the PSRs 2017 on when an ASPSP may not refuse to execute an authorised payment order).

17.~~36~~44 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.~~37~~45 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~~/~~ or 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. In our view, however, 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.~~38~~46 Authorisation or registration as an AISP or PISP does not allow a business to access customer account data or payments functionality where no AIS or PIS is being provided. Each time an AISP or PISP uses its regulatory status, or the eIDAS certificate it is issued (see 17.60 below), to access a customer account, it must be for the purpose of providing an AIS or PIS to that customer.

17.47 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. If, however, providing this information would compromise reasonable security measures, or would be unlawful (e.g. if it would constitute 'tipping off' under anti- money laundering legislation) this requirement does not apply. For more details see the guidance at paragraph 19.20 in **Chapter 19 – Financial crime**).

17.~~39~~48 The ASPSP must restore access to the AISP or PISP as soon as the reasons for denying access no longer exist.

17.~~40~~49 Under regulation 71(8) of the PSRs 2017, whenever an ASPSP denies an AISP or a PISP access to a payment account (or payment accounts) for reasons relating to unauthorised or fraudulent access it must notify us immediately. This notification requirement does not apply where payment orders or information requests made through AISPs or PISPs are refused for legitimate reasons which would have led the ASPSPs to refuse those orders or requests from the customer themselves (as set out in paragraph 17.~~34~~42). 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.~~41~~50 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.~~42~~51 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 provide further guidance on ~~AISPs~~ AISPs' and PISPs' obligations in relation to sensitive payment data (which include personalised security credentials) in paragraphs 17.~~51~~62 – 17.~~54~~65.

17.~~43~~52 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), 68(5)(b), 69(2), 69(3)(c) and 70(3)(a))

17.~~44~~53 AISPs must not provide AIS without the customer's 'explicit consent' to do so. Similarly, a customer's 'explicit consent' is required for the execution of a payment transaction through a PISP. PISPs must not pass information to any person except a payee and then only with the payer's 'explicit consent'. CBPIIs must have obtained the 'explicit consent' of the customer before they begin to request confirmation of availability of funds. We expect CBPIIs, PISPs and AISPs to be able to evidence their customers' explicit consent.

17.~~45~~54 The requirement to obtain 'explicit consent' under regulations 68, 69 and 70 of the PSRs 2017 is distinct from any obligations a PSP has under data protection law. A PSP must ensure that it meets its obligations under both the PSRs 2017 and data protection law cumulatively. See paragraphs 8.52 – 8.~~59~~56 in **Chapter 8 – Conduct of business requirements** for further details regarding data protection law.

17.~~46~~55 In order to enable customers to give 'explicit consent' in accordance with the PSRs 2017, in our view AISPs and CBPIIs 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 consent should be clear and specific. For AISPs, aside from any requirements of data protection legislation, we consider this to include information about how the ~~customer's~~customer's payment account information will be used and whether any other parties will have access to that information. It is the ~~AISP~~AISP's or CBPII's responsibility to ensure that the customer has received sufficient information in order to give explicit consent.

17.~~47~~56 In the case of PIS, explicit consent for the execution of the payment transaction is given in accordance with regulation 67 of the PSRs 2017 (further information can be found in paragraphs 8.54 – 8.55). In our view, where a customer gives this explicit consent through a PISP, this will also be sufficient evidence of the customer's explicit request for the PISP to provide the payment initiation service, as required by regulation 69(3)(g) of the PSRs 2017.

17.~~48~~ 57 Where a payment order requires authentication by more than one party (for example, in the case of a business where payments above a certain amount need to be approved by a second or more senior employee), the same legal obligations apply. Collection of the multiple authentication elements may be undertaken by the PISP where it is feasible to do so, or by the ASPSP. Any redirection to the ASPSP must be for the purpose of authentication only (see paragraphs 17.125 and 17.126 below), i.e. to confirm that the appropriate parties authorise the payment order. The ASPSP may not allow any authenticating party to change the payment order without going through the PISP.

17.58 In line with the EBA Opinion, ASPSPs are not required to check the terms of the consent provided by the customer to AISPs, PISPs or CBPIIs~~, nor~~. Nor, in our view, are they able to seek proof, or confirmation from the customer, of that consent as a prerequisite to fulfilling their obligations to provide access to AISPs, PISPs or CPBIIs. Where an ASPSP is involved in authentication of an AIS request or PISP initiated payment, it should ensure that its involvement does not directly or indirectly dissuade customers from using the services of PISPs, AISPs or CBPIIs. ASPSPs have a separate obligation to obtain the customer's 'explicit consent' before responding to CBPII requests for confirmation of availability of funds (see paragraph 8.164 of **Chapter 8 – Conduct of business requirements** for further details).

Identification and communication with the ASPSP (~~regulation~~regulations 68(3) (c), 69(3)(d)~~and~~ and 70(3)(c))

17.~~49~~59 Regulation 68(3)(c), 69(3)(d) and 70(3)(c) of the PSRs 2017 apply ~~18 months after~~from 14 September ~~the SCA-RTS is published in the Official Journal of the European Union.~~2019. Once this happens, in accordance with SCA-RTS Article 30(1)(a) both AISPs and PISPs must identify themselves to the ASPSP each time they initiate a payment order or for each communication session (see also section 17.90 to 17.96). CBPIIs must ~~authenticate~~ identify themselves towards the ASPSP before each confirmation request. ~~We expect the~~There is no ~~SCA-RTS to set out how such identification or confirmation must take place.~~

~~**17.50**~~requirement for the ASPSP to identify itself towards the CBPII, PISP or AISP. However, we encourage mutual authentication to take place as part of a secure communication session.

17.60 SCA-RTS Article 34 requires CBPIIs, PISPs and AISPs to identify themselves towards the ASPSP using qualified certificates issued by Qualified Trust Service Providers. SCA-RTS Article 30(1)(a) requires ASPSPs to have in place at least one interface that enables this identification to take place. CBPIIs, PISPs and AISPs must ensure that the qualified certificates, used for identification for the purpose of the payment ser vice provided, accurately reflect that PSP's role and authorisation or registration status at all times. ASPSPs should accept qualified certificates presented by agents or outsource providers acting on behalf of AISPs, PISPs and CBPIIs, provided that the ASPSP is in a position to unequivocally identify the principal PSP in the presented certificate. Additional clarification is provided in the EBA Opinion on the use of eIDAS certificates under the SCA-RTS.[60] ASPSPs should meet the contingency mechanism requirement to ensure identification (SCA-RTS Article 33(5)) through accepting qualified certificates.

17.61 CBPIIs, PISPs and AISPs are also obligated to communicate in accordance with the SCA-RTS. ~~We expect the~~ SCA-RTS ~~to~~Articles 28 to 36 contain a number of requirements in relation to the method of communication used by the CBPII, PISP and AISP, as well as security measures that they must apply whenever they communicate with ASPSPs and with the customer. In relation to whichever method of access AISPs~~/~~, PISPs~~/~~ and CBPIIs use,

60 See https://eba.europa.eu/documents/10180/2137845/EBA+Opinion+on+the+use+of+eIDAS+certificates+under+the+RTS+on+SCACSC.pdf

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). Further guidance on AISPs~~, PISPs~~', PISPs' and CBPIIs' obligations before the SCA-RTS apply can be found in paragraphs 17.~~66~~80-17.~~71~~85.

Sensitive payment data (regulations 69(3)(e) and 70(3)(e))

17.~~51~~62 PISPs are not permitted to store sensitive payment data of the customer. AISPs are not permitted to request sensitive payment data linked to the payment accounts they access.

17.~~52~~63 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.~~53~~64 For AISPs, in our view:

- we would not generally expect this prohibition to limit the ability of AISPs to provide consolidated account information to a customer;
- where use of the customer's personalised security credentials is necessary for the AISP to provide AIS, the AISP can store the personalised security credentials if the AISP has obtained them directly from the customer, rather than requesting them from the ASPSP.

17.~~54~~65 For PISPs, in our view:

- this prohibition primarily means that PISPs must not store a customer's personalised security credentials once they have used them for the purposes of initiating a payment transaction;

- the prohibition has no effect where the PISP legitimately holds the sensitive payment data in question by virtue of providing the payer with another payment service, e.g. where an ASPSP is also an AISP ~~/~~ or PISP. The PISP is not, however, permitted to use sensitive payment data obtained or held for the purposes of the other payment service (including AIS) when it is providing the PIS.

Using, accessing and storing information (regulations 68(8)(a), 69(3)(g) and 70(3)(f))

17.~~55~~66 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.~~56~~67 Under SCA-RTS Article 36(3), AISPs must have in place suitable and effective mechanisms to prevent access to information other than from designated payment accounts and associated payment transactions, in accordance with the user's explicit consent. This means that where a customer only provides explicit consent to the AISP for a sub-set of their account data to be accessed (e.g. their current account but not their credit card account), only this should be accessed by the AISP.

17.68 The PSRs 2017 do not prohibit PISPs from using and storing the payment service user's account number and sort code for the purpose of providing a payment initiation service, with the customer's explicit consent.

17.69 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. confirmation that the payment has been made) made directly by the payer.

17.~~57~~70 For AISPs in particular, this will depend on the nature of the service. For example, an AISP providing detailed analytics of a customer's spending habits would need to access more information than an AISP providing a service which frequently updated the customer on their balances on various accounts.

17.~~58~~71 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 the SCA-RTS, applicable data protection law, SYSC and other systems and control requirements.

17.~~59~~72 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.~~60~~73 A PISP must not hold the payer's funds in connection with the provision of the PIS at any time.

Requesting information (regulation~~s~~ 69(3)(f))

17.~~61~~74 PISPs are not permitted to request any information from the payer except information required to provide the payment initiation service. As a general principle, we take this to mean that PISPs should not request more information than is absolutely necessary to provide the specific service that they offer to their customers. For example, we would not expect PISPs acting on behalf of merchants for single payment transactions to need information on a customer's other transactions or balance. The exception to

this, in line with the EBA Opinion, is that the PISP may request certain information, in certain circumstances, to manage execution risk. See section 17.24 above.

Not changing the payment order (regulation 69(3)(h))

17.~~62~~75 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.~~63~~76 AISPs must not access any information other than information from designated payment accounts and associated payment transactions and are required to have in place suitable and effective mechanisms to ensure this is the case in accordance with SCA-RTS Article 36(3). This is intended to give customers control over what is being accessed by an AISP. This requirement does not prohibit AISPs from accessing

accounts which are out of scope of the PSRs 2017 ie non-payment accounts (for example, some savings accounts. See PERG 15.3 Q.16).

17.77 As stated in SCA-RTS Article 36(5), AISPs are permitted to access account information from designated payment accounts whenever the payment service user actively requests such information. In our view, in line with the EBA Opinion, an active request requires the payment service user to be actively viewing the data or executing an action to refresh the data to be displayed. In the absence of the active involvement of the payment service user, access is restricted to no more than four times a day unless more frequent access is agreed between the AISP and ASPSP, with the customer's consent. Such a bilateral arrangement could also involve an agreement whereby the ASPSP will push information to the AISP, subject to the customer's consent.

Requirements on ASPSPs, CBPIIs, PISPs and AISPs when communicating and interacting with their customers in relation to these services

17.~~64~~78 In **Chapter 8 – Conduct of business requirements** 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, how information will be used, and how to make a complaint – see paragraph 8.117 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 8.81 of **Chapter 8 – Conduct of business requirements**.

17.~~65~~79 ASPSPs, CBPIIs, AISPs and PISPs also need to be aware of their obligations under data protection law (see paragraphs 8.52 – 8.~~59~~56 of **Chapter 8 – Conduct of business requirements**) and under consumer protection law, such as the Consumer Protection from Unfair Trading Regulations 2008 which prohibit unfair, misleading and aggressive practices (see paragraphs 8.34 – 8.45 of **Chapter 8 – Conduct of business requirements**).

Transitional arrangements before the SCA-RTS becomes applicable

Communication and methods of access

17.~~66~~80 In relation to certain provisions, there is a transitional period beginning on 13 January 2018~~ and ending 18 months after the date~~, which will end when the SCA-RTS enters into ~~force.~~ effect on 14 September 2019.

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), 77(4)(c) and (6) and 100 which depend on the SCA-RTS~~ and~~ and start to apply at the same time as the SCA-RTS.

17.~~67~~81 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 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.~~68~~82 From 13 January 2018, ASPSPs can deny an AISP or PISP access to a payment account only if the conditions in regulation 71(7) of the PSRs 2017 are met (see paragraphs 17.~~34 –~~42 – 17.~~40~~49). 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 appropriate.

17.~~69~~83 In advance of the date on which the SCA-RTS becomes applicable, an ASPSP is not required to provide a method of access that meets the requirements of the SCA-RTS. If an ASPSP chooses to put in place a method of access complying with the SCA-RTS before that date, the ASPSP must not block or obstruct the provision of regulated AIS and PIS, by making early compliance with the specific requirements that depend on the SCA-RTS a prerequisite for access by AISPs or PISPs. As a result, during the transitional period, the ASPSP will have to permit AISPs and PISPs to use the method of access (e.g. the online banking portal) offered by the ASPSP to its customers or provide another method of access which AISPs and PISPs can use without having to comply with requirements yet to come into force~~, e.g. the requirement that they must identify themselves as part of each communication session or payment order~~.

17.~~70~~84 Where an ASPSP provides a method of access which complies fully with the PSRs 2017 during the transitional period (including the obligation to treat data requests and payment orders in the same way as those that come directly from their customer unless it has objective reasons to treat them differently), the ASPSP is not required to provide or permit an alternative method of access to those payment accounts.

17.~~71~~85 During the period before the SCA-RTS becomes applicable, the parties may find it helpful to take account of ~~standards[50]~~standards[61] which are being developed as a result of the Competition and Markets Authority's Open Banking Remedy.[~~51~~62]

Businesses providing AIS or PIS before 12 January 2016

17.~~72~~86 We have provided guidance in **Chapter 3 – Authorisation and registration** and PERG 15.7 on the timeframes in which businesses that were providing PIS or AIS before 12 January 2016 and continuing to do so immediately before 13 January 2018 will need to be authorised or registered.

17.~~73~~87 Until these businesses are authorised or registered, as appropriate, they will be treated for the purposes of the PSRs 2017 or the EMRs 2011 as if they were not providing PIS or AIS. As a result, ASPSPs will not be obligated to allow them access to customers' payment accounts.

17.~~74~~88 Providers of PIS and AIS that are not authorised or registered should not mislead customers about their regulatory status by implying that they have been authorised or registered by the FCA.

~~50~~

61 More information on Open Banking delivery can be found here: https://www.openbanking.org.uk/ ~~https://www.openbanking.org.uk/2017/03/13/platform-distributing-bank-product-branch-atm-data-available/~~

~~51~~62 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

HM Treasury and FCA Expectations for the third party access provisions in PSD2

17.~~75~~89 HM Treasury and the FCA issued a joint communication in July ~~2017~~2017[63] outlining our expectations for AISPs, PISPs and ASPSPs during the transitional period before the SCA-RTS becomes applicable. We also provide further information on our approach to registration and authorisation, including for businesses that provided AIS or PIS before 12 January 2016. All providers should have regard to this communication, which can be found on HM Treasury's website.~~52~~[64]

Requirements on all ASPSPs for secure communication

17.90 From 14 September 2019, all ASPSPs must comply with requirements in the SCA-RTS for secure communication with AISPs, PISPs and CBPIIs. The requirements concern how ASPSPs and AISPs, PISPs and CBPIIs should communicate with one another via the ASPSP's 'access interface'.

52

17.91 SCA-RTS Article 31 outlines the access interface options. An ASPSP can provide access:

- by allowing the use by AISPs, PISPs and CBPIIs of the interfaces used for authentication and communication with the ASPSP's customers or
- via a 'dedicated interface'

17.92 We encourage ASPSPs to make use of application programming interfaces (APIs) in order to provide dedicated interfaces. As we confirmed in our joint statement with HM Treasury, we support implementation of PSD2 using such APIs. Where developed according to common standards and using secure common infrastructure, APIs can support innovation by reducing barriers to entry – as third parties will not have to integrate with different technology on a firm-by-firm basis – and can enhance security across the industry. That said, ASPSPs are not required to follow particular common standards. Furthermore, it is for individual ASPSPs to ensure their implementation of particular API standards enables them to meet the requirement of PSD2 and the SCA-RTS.

17.93 Regardless of which access interface option is chosen, PSPs (ASPSPs, PISPs, AISPs and CBPIIs) are required to comply with the relevant obligations set out in SCA-RTS Articles 30 (general obligations for access interfaces), 34 (certificates), 35 (security of communication session) and 36 (data exchanges).

17.94 It is important to note that all ASPSPs must meet the requirements set out in SCA-RTS Article 30 to make available both technical specifications regarding their interface, and testing facilities by 14 March 2019.

Allowing the use by AISPs, PISPs and CBPIIs of the interfaces used for authentication and communication with the ASPSP's customers ('the modified customer interface')

17.95 An ASPSP can choose to provide access via the interfaces used for authentication and communication with the ASPSP's customers. However, this interface will need to be modified to meet SCA-RTS requirements. The 'modified customer interface' must meet requirements in SCA-RTS Article 30. This includes, but is not limited to:

63 The joint statement is available here: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/630135/Expectations_for_the_third_party_access_provisions_in_PSDII.pdf

64 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/630135/Expectations_for_the_third_party_access_provisions_in_PSDII.pdf

identification, secure communication and allowing AISPs and PISPs to rely on all the authentication procedures provided by the ASPSP to the customer.

17.96 The 'modified customer interface' must also comply with SCA-RTS Articles 34 (certificates), 35 (security of communication session) and 36 (data exchanges).

Requirements on ASPSPs providing access via a dedicated interface

Contingency measures under SCA-RTS Article 33

17.97 Where an ASPSP chooses to provide access via a dedicated interface, it must have contingency measures in place that come into effect when the conditions in SCA-RTS Article 33(1) are met. The conditions include that:

- the interface does not perform in compliance with Article 32
- there is unplanned unavailability of the interface or a systems breakdown

17.98 Unplanned unavailability or a systems breakdown may be presumed to have arisen when five consecutive requests for access to information for the provision of payment initiation services or account information services are not replied to within 30 seconds. This should be distinguished from a situation where account access is blocked due to consecutive failed authentication attempts in accordance with SCA-RTS Article 4(3)(b) (see **Chapeter 20 – Authentication** section 20.31). In the latter scenario, we expect ASPSPs to communicate to AISPs and PISPs the reason why access has been blocked. ASPSPs must notify the payment service user of the denial of access (see 17.42 to 17.49). Furthermore, Article 4(4) requires the ASPSP to alert the payment service user if the block is made permanent.

17.99 The contingency measures cover:

- having a strategy and plans in place for when the dedicated interface stops complying with the requirements of SCA-RTS Article 32, or there is unplanned unavailability of the interface or a systems breakdown (SCA-RTS Article 33(1))
- having communication plans (SCA-RTS Article 33(2))
- having a 'contingency mechanism' in place (SCA-RTS Article 33(4)).

The contingency mechanism

17.100 Broadly, the contingency mechanism requirements are intended to ensure that if an AISP or PISP cannot access a customer's payment account via the dedicated interface (due to unavailability), it can, instead, access through the online interface(s) the customer has with their ASPSP. Reliance on the contingency mechanism should be a temporary measure, until the dedicated interface is restored to the required level of availability and performance (see SCA-RTS Article 32) or the ASPSP has implemented the modified customer interface.

17.101 Where the contingency mechanism is relied upon, the ASPSP must ensure it meets the requirements in SCA-RTS Article 33. This includes providing a means for the AISP or PISP to be identified (this must be through the use of certificates – see section

17.60 on certificates) and ensuring the AISP or PISP can rely on the authentication procedures provided by the ASPSP to the customer.

Exemption from the contingency mechanism

17.102 The SCA-RTS allows competent authorities to exempt ASPSPs from the obligation to provide a contingency mechanism. It should be noted that this does not exempt ASPSPs from the broader contingency measures in SCA-RTS Article 33(1) and 33(2).

17.103 Under SCA-RTS Article 33(6) the FCA, after consultation with the EBA, is required to exempt ASPSPs from the requirement to provide a contingency mechanism if the ASPSP can demonstrate to the FCA that it has met certain conditions. The FCA will meet this requirement in line with the EBA's Guidelines on the conditions to benefit from an exemption from the contingency mechanism under Article 33(6) of Regulation (EU) 2018/389 ("the EBA Guidelines").[65] The table below sets out how the EBA Guidelines relate to the SCA-RTS Article 33(6) requirements for exemption:

SCA-RTS critiera	Relevant EBA Guideline(s)
Article 33(6)(a) The dedicated interface complies with all the obligations for dedicated interfaces as set out in Article 32	EBA Guidelines 2: Service level, availability and performance EBA Guideline 3: Publication of statistics EBA Guideline 4: Stress testing EBA Guideline 5: Obstacles
Article 33(6)(b) The dedicated interface has been designed and tested in accordance with Article 30(5) to the satisfaction of the payment service providers referred to therein	EBA Guideline 6: Design and testing to the satisfaction of PSPs
Article 33(6)(c) The dedicated interface has been widely used for at least 3 months by payment service providers to offer account information services, payment initiation services and to provide confirmation on the availability of funds for card-based payments;	EBA Guideline 7: Wide usage of the interface
Article 33(6)(d) Any problem related to the dedicated interface has been resolved without undue delay.	EBA Guideline 8: Resolution of problems

Requesting exemption from the contingency mechanism under SCA-RTS Article 33(6)

17.104 ASPSPs wishing to request exemption from the contingency mechanism requirement need to complete an exemption request form and submit it to us. Exemption request forms are available after registering on Connect. There is no fee associated with submitting this form. The form can be viewed in SUP 15C Annex 1. An ASPSP that wishes to passport, whether by establishing a branch, or providing cross border ser vices, should submit its exemption request to its home state regulator.

17.105 Where a group of ASPSPs or a single ASPSP operates a number of different dedicated interfaces, e.g. in respect of different banking brands, subsidiaries or products, we

65 https://eba.europa.eu/documents/10180/2250578/Final+Report+on+Guidelines+on+the+exemption+to+the+fall+back.pdf

require separate requests in respect of each different dedicated interface for which an ASPSP is seeking an exemption. Where a group of ASPSPs operates the same dedicated interface across different banking brands, we require a single request for that dedicated interface.

17.106 An ASPSP that intends to provide access to some of its online payment accounts via its dedicated interface, and intends to modify the customer interface for its remaining online payment accounts, may still seek exemption for its dedicated interface. All of its online payment accounts must be accessible in an SCA-RTS compliant manner.

Information to be provided and EBA guidelines

17.107 The EBA Guidelines, addressed to competent authorities and to PSPs, clarify the conditions which the FCA should assess as having been met in order to exempt ASPSPs.

17.108 From section 17.112 onwards we provide guidance on the information we will require from ASPSPs in order to make an assessment of whether the criteria in the SCA-RTS and conditions in the EBA Guidelines have been met.

Processing exemption requests

17.109 We will acknowledge that we have received an exemption request. We will assess the information provided against the conditions set out in the EBA Guidelines. Where exemption requests are incomplete (when they do not include all the information we need), we will ask for more information.

Decision making process

17.110 Once we are satisfied that all the information required as part of an exemption request has been provided (ie the request is complete), we will aim to determine whether to grant the exemption within one calendar month. We will notify the ASPSP of the exemption decision in writing.

17.111 Where an ASPSP's dedicated interface does not meet a small number of the legal requirements necessary for an exemption at the point the exemption request is submitted, we may nevertheless indicate that we are 'minded to exempt' if the ASPSP has clear and credible plans to meet these requirements in time for 14 September 2019. We will confirm the exemption once we have received information that satisfies us that all PSD2 requirements are met.

Exemption criteria and FCA information requirements

17.112 In order to assess whether the conditions of the EBA Guidelines are met, we require ASPSPs to provide the information set out below using Form A and Form B specified in *SUP 15C Annex 1*. Each information requirement in Form A has a question number (e.g. Q1). Form B is specific to EBA Guideline 6 and the design of the interface.

Service level, availability and performance (EBA Guideline 2)

17.113 EBA Guideline 2 concerns the conditions for meeting the requirement that the dedicated interface has the same or better levels of availability and performance as the interface(s) that customers use to access their payment accounts directly. This must be measurable, so the EBA Guidelines set out what ASPSPs should measure for

availability and performance, and how availability indicators should be calculated. To assess whether the criteria are met, we require the following information:

Q1: Confirmation that the ASPSP has defined service level targets for out of hours support, monitoring, contingency plans and maintenance of its dedicated interface that are at least as stringent as those for the interface(s) used by its own payment service users. We may ask ASPSPs to provide supporting evidence.

Q2: Confirmation that the ASPSP has put in place measures to calculate and record performance and availability indicators in line with EBA Guidelines 2.2 – 2.4.

Publication of statistics (EBA Guideline 3)

17.114 EBA Guideline 3 concerns the requirement for publication of quarterly statistics on the availability and performance of the dedicated interface. The EBA Guidelines set out what ASPSPs should provide to the FCA, in order for us to assess whether this criterion is met. We require the following information:

Q3: A plan for the quarterly publication of daily statistics required under SCA-RTS Article 32(4) and in line with EBA Guideline 3.

17.115 This plan should include:

- confirmation that the publication each quarter will present daily availability and performance statistics (measured and calculated as per EBA Guideline 2)
- the planned date of the first publication (although the SCA-RTS does not give details of what quarterly means in terms of publication of the statistics, we would expect the publication to align to standard calendar quarters)
- a brief description of where the statistics will be published on the ASPSP's website (including the URL)
- a brief description of how the publication will enable the comparison of the availability and performance of the dedicated interface with that of each of the interfaces made available by the ASPSP to its payment service users on a daily basis.

17.116 The statistics should be published in a clear and understandable format. We agree with the EBA[66] that publishing in a line chart format to display both statistics of the dedicated interface and customer interfaces in the same chart may facilitate comparison between the dedicated interface and the customer interface. However, we note that the underlying statistics should be available to visitors to the website (for example, available to download or view). We also encourage ASPSPs to locate these statistics in an accessible part of the website, and in close proximity to webpages covering service metrics required under BCOBS 7 (information on current account services)[67] where these service metric rules apply.

66 Final Report: Guidelines on the conditions to benefit from an exemption from the contingency mechanism under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC) feedback table row 39

67 https://www.fca.org.uk/publication/policy/ps17-26.pdf

17.117 ASPSPs should note that we have required all ASPSPs to report these quarterly published statistics to the FCA. More information about how to submit this reporting can be found in **Chapter 13 – Reporting and notifications** and SUP 16.13.

Stress testing (EBA Guideline 4)

17.118 EBA Guideline 4 concerns the conditions for meeting stress testing requirements. ASPSPs should have in place processes to establish and assess how the dedicated interface performs when subjected to an extremely high number of requests from PISPs, AISPs and CBPIIs, in terms of the impact that such stresses have on the availability and performance of the dedicated interface and the defined service level targets. EBA Guideline 4.2 a-d sets out the capabilities that should be tested as a minimum.

17.119 We are primarily concerned that once in operation with AISPs, PISPs and CBPIIs, the ASPSP's dedicated interface will be able to handle large volumes of requests (of differing complexity) by AISPs, PISPs and CBPIIs. The stress testing should be able to demonstrate that performance and availability of the interface will not be adversely affected by events that create stresses on the system. ASPSPs' stress testing may take into account the relative size of the firms likely to access accounts and the likely number of their customers. We encourage ASPSPs to engage with AISPs, PISPs and CBPIIs to understand and forecast when peak usage or other stresses may occur in order to undertake adequate stress testing.

17.120 In order to assess whether this criterion is met, we require the following information:

Q4: A summary of the results of stress tests undertaken as per EBA Guideline 4.

17.121 This summary should cover, as a minimum:

- results of the stress testing of the capabilities set out in EBA Guideline 4.2 a-d
- the assumptions used as a basis for stress testing each of these capabilities (for example, how the ASPSP came to define what an extremely large number of requests would be)
- how any issues identified during stress testing have been addressed

Obstacles (EBA Guideline 5)

17.122 EBA Guideline 5 concerns the conditions for assessing that an ASPSP's dedicated interface does not create obstacles to the provision of payment initiation and account information services.

17.123 In order to assess whether an ASPSP's dedicated interface creates any such obstacles, we require an ASPSP to provide the following information:

Q5: A description of the method(s) of carrying out the authentication procedure(s) of the customer that are supported by the dedicated interface.

17.124 For each method of carrying out the authentication procedure, this should comprise of:

- a summary of the authentication procedure
- an explanation of why the authentication procedure does not create obstacles
- supporting evidence such as screenshots, walkthroughs or videos of the customer journey and evidence concerning, for example, usage of the interface (e.g. successful calls on API) and customer drop-out rates

Guidance on the information to be provided for Q5 – 'summary of the authentication procedure(s)'

17.125 The EBA's Opinion[68] describes different methods of carrying out authentication procedure(s), including 'redirection', 'decoupled' and 'embedded' methods.

17.126 'Redirection' has been described by the EBA[69] as 'a process whereby once consent has been given to the AISP or PISP to access a customer's account for the purpose of an AIS or PIS, the customer is 're-directed automatically to the ASPSP's domain (webpage or application) for the purpose of entering the ASPSP-issued credentials to complete authentication. The customer is then directed back to the AISP/PISP domain for the completion of the process'.

17.127 The FCA's understanding of 'decoupled' (also known as out-of-band authentication) is that it allows the customer to complete the authentication procedure on a separate device to the device on which the AISP or PISP's app or website is being used. For example, if paying online via a PISP using a desktop browser, decoupled authentication would allow a customer to authenticate using a banking app on a mobile phone. This is a form of redirection because the customer is being redirected to their ASPSP's domain (on another device) in order to authenticate.

17.128 The FCA's understanding of 'embedded' authentication is that it allows for a customer's ASPSP-issued credentials to be given directly to the AISP or PISP. The customer does not interact with its ASPSP to complete authentication where the ASPSP offers the embedded access method.

17.129 The summary of the authentication procedure for Q5 should specify which of the above described authentication methods best describes the method(s) chosen and include a description of the flow of authentication data (credentials) from the customer to the ASPSP and, where relevant, at which point, if at all, the AISP or PISP comes into possession of the authentication data or credentials.

Guidance on information to be provided for Q5 – 'explanation of why the methods of carrying out the authentication procedure do not create obstacles'

17.130 For each access method provided, we require an explanation of the reasons why the method is not an obstacle. We provide guidance below on each of the four obstacles described in SCA-RTS Article 32(3):

68 EBA Opinion section 48

69 EBA Consultation paper: Draft Guidelines on the conditions to be met to benefit from an exemption from contingency measures under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC) https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-the-conditions-to-be-met-to-benefit-from-an-exemption-from-contingency-measures-under-article-33-6-of-regulation-eu-2018/389-rts-on-sca-csc-

- *preventing the use by payment service providers referred to in Article 30(1) of the credentials issued by account servicing payment service providers to their customers*

17.131 Under regulation 100(4) of the PSRs 2017, an ASPSP must allow a PISP or AISP to rely on the authentication procedures provided by the ASPSP to a customer.

17.132 ASPSPs should consider all customer credentials and authentication procedures and the combinations of those credentials and procedures in which the ASPSP permits customers to authenticate themselves and consider how the customer experience is managed for customers when accessing payment accounts via an AISP or PISP. For example, if a customer can authenticate using fingerprint biometrics when accessing their account directly, this should be available as an authentication method when the customer is accessing their account through an AISP or PISP.

17.133 An explanation should be given when completing Q5, if authentication methods that the customer can use when directly accessing their account are not available to the customer when accessing their payment account through an AISP or using a PISP.

17.134 In our view where an interface redirects the payment service user to the ASPSP for authentication, an AISP or PISP is not prevented from relying on the ASPSP- issued credentials. This is because the AISP or PISP is able to rely upon the ASPSP authentication procedures, which include the use of the ASPSP-issued credentials by the payment service user, when they are redirected to the ASPSP. Furthermore, the AISP or PISP is not required to issue its own credentials or authentication procedures.

- *imposing redirection to the account servicing payment service provider's authentication or other functions*

17.135 In our view, in line with the EBA Opinion, the SCA-RTS do not state that redirection per se is an obstacle for AISPs and PISPs to provide services to their customers. Instead, the SCA-RTS states that it "may" be so, if the ASPSP implements it in a manner which is restrictive or obstructive for AISPs or PISPs.

17.136 AISPs and PISPs must be able to rely on all of the authentication procedures provided by the account provider to the customer, without the addition of any unnecessary steps that might cause delay. Any steps arising from the ASPSP's implementation of redirection, which go beyond what is required for PSD2 and the SCA-RTS, should be specifically justified when completing the explanation in Q5.

17.137 ASPSPs implementing redirection should note that we are not aware of any reason for ASPSPs to request strong customer authentication more than once when facilitating authentication for a single session of access to account information or a single payment initiation. For PIS, obtaining strong customer authentication once is compatible with dynamic linking requirements. The ASPSP should generate the authentication code based on the amount and payee transmitted securely to the ASPSP by the PISP, which will have been consented to by the payer.

17.138 In the context of redirection, the functionality provided directly to the customer via different channels (e.g. mobile app or desktop browser) should not determine the method of authentication available to a customer when using an AISP or PISP. For example, the fact that a customer cannot set up a new payee using the ASPSP mobile

app, should not prevent app based authentication when a PISP is used i.e. to set up a new payee.

- *requiring additional authorisations and registrations in addition to those provided for in Articles 11, 14 and 15 of PSD2*

17.139 Once authorised or registered, AISPs and PISPs have a right to access customer payment accounts, with the customer's explicit consent. Under PSD2 and the SCA-RTS, the ability to access a customer's payment account should not be contingent on anything other than the AISP or PISP having been authorised or registered by the FCA or another competent authority (acknowledging that the AISP or PISP must identify itself to the ASPSP so this can be confirmed).

17.140 Some initiatives involve certain steps being taken by PISPs, AISPs and CBPIIs, in order for them to use standardised APIs to access payment accounts via dedicated interfaces, such as enrolment in an API programme (eg that run by the Open Banking Implementation Entity (OBIE) in the UK). In our view, the SCA-RTS does not preclude the possibility for an ASPSP to require PISPs, AISPs or CBPIIs to complete such steps, as long as such steps are in line with the above guidance.

17.141 Under Q5, ASPSPs should explain any additional authorisation or registration steps imposed on AISPs, PISPs or CBPIIs, or any API enrolment steps, with an explanation of what those steps entail and why those steps do not impose obstacles.

- *requiring additional checks of the consent given by payment service users to providers of payment initiation and account information services.*

17.142 ASPSPs are not required to check the terms of the consent provided by the customer to AISPs, PISPs or CBPIIs. Nor, in our view, are they able to seek proof, or confirmation from the customer, of that consent as a prerequisite to fulfilling their obligations to provide access to AISPs, PISPs or CPBIIs. The FCA will not grant an exemption in respect of interfaces that include such additional steps. An ASPSP asking the customer to confirm that they agree to share data with an AISP will be considered an example of an additional consent step. The FCA will carefully scrutinise any aspect of an ASPSP's dedicated interface that gives rise to messaging or steps that go beyond facilitating authentication or specific legislative or regulatory requirements.

17.143 Where an ASPSP's dedicated interface provides for redirection this should be for authentication purposes only. Redirection from the AISP to the ASPSP should not be used by the ASPSP as an opportunity to gather additional consent or authorisation from the customer in order to allow the AISP access to the payment account for the purpose of providing AIS. We encourage ASPSPs to make sure redirection to the ASPSP is a coherent part of the customer journey which will begin and end with a customer interacting with an AISP or PISP.

17.144 Similarly, in the FCA's view, where explicit consent has been given to a PISP to initiate a payment order with respect to a payment account held at another PSP the customer does not need to confirm that consent has been given to the PISP in order for PIS to be provided.

17.145 In cases where a customer has more than one account with an ASPSP, account selection may be carried out between the customer and AISP or the PISP, or, if not feasible, with the ASPSP. If the PISP or AISP can inform the ASPSP which account(s)

have been selected, together with the payment initiation or account information request, the ASPSP should not require the customer to select the account again before executing the PISP's request. If, however, the account selection can only take place in the ASPSP's domain, this will not amount to an obstacle to the provision of AIS or PIS.

17.146 It should be noted that consent for the purposes of authorisation of a payment transaction can be given via the PISP (regulation 67(2)(c) of the PSRs 2017). This will be the case where there is no redirection.

Guidance on evidencing that the dedicated interface does not dissuade customers through unnecessary delays or friction

17.147 Under EBA Guideline 5, ASPSPs should also provide evidence that the dedicated interface does not give rise to unnecessary delay, friction or any other attributes that would mean that customers are directly or indirectly dissuaded from using the services of PISPs, AISPs and CBPIIs.

17.148 In our view, customers may be dissuaded, for example, if they are accustomed to authenticating using biometrics via the banking application ('app') on a mobile phone, but are prevented from doing this as part of the authentication journey when accessing accounts via an AIS or PIS. Customers may also be dissuaded if the customer journey is cumbersome, for example, if they are required to provide strong customer authentication multiple times in a single session of access to account information or a single payment initiation. We are not aware of any reasons for ASPSPs to request strong customer authentication more than once when facilitating authentication for a single session of access to account information or a single payment initiation.

17.149 ASPSPs should submit supporting evidence of customer journeys, for each access method, in the form of screenshots, walkthroughs or videos of the customer journey and evidence concerning, for example, usage of the interface (e.g. successful calls on API) and customer drop-out rates. Evidence of consumer testing or alignment to market initiative specifications that have had the input of consumers will also be a relevant consideration in our assessment.

Design and testing to the satisfaction of PSPs (EBA Guideline 6)

17.150 EBA Guideline 6 concerns requirements for the design and testing of the dedicated interface to the satisfaction of the payment service providers.

Design

17.151 Under EBA Guideline 6.1, ASPSPs need to provide evidence that the dedicated interface meets the legal requirements for access and data in PSD2 and the SCA-RTS. For this purpose, we have provided 'Form B' in SUP 15C Annex 1 based on the main requirements for dedicated interfaces and API initiatives set out in Table 1 in the EBA Opinion. Against each of the main requirements for access interfaces, ASPSPs should provide:

- a description of the functional and technical specifications that the ASPSP has implemented

- a summary of how the implementation of these specifications fulfils the requirements in PSD2 and the SCA-RTS

17.152 Where certain requirements are not being met when the exemption request is submitted, an ASPSP should provide the date by when the relevant functionality

will be implemented. As noted in 17.111, we may nevertheless indicate that we are 'minded to exempt' if the account provider has clear and credible plans to meet these requirements in time for 14 September 2019. Exemption will only be confirmed once we are satisfied that the legal requirements and criteria have been met.

17.153 EBA Guideline 6.2 sets out that an ASPSP may provide information about standards it has implemented that have been developed by a market initiative. An ASPSP should provide this information, where relevant, in Form B as part of its description of the functional and technical specifications, and how these meet PSD2 standards.

17.154 We expect that in the development of API standards, initiatives such as the Open Banking Implementation Entity (OBIE) will have undertaken extensive engagement with different market participants towards ensuring APIs work well. We also expect extensive work to have been undertaken to ensure the standards are aligned with PSD2 legal requirements. Nonetheless, it remains the ASPSP's responsibility to ensure this is the case with respect to any standards used. We note that as part of their work, initiatives[70] may facilitate conformance testing (also known as compliance testing) of dedicated interfaces against their specified API standards as well as against PSD2 legal requirements. Information about the results of any conformance testing, and any deviation from the initiative standard should be provided using Form B.

17.155 In addition to Form B, under EBA Guideline 6, we require ASPSPs to provide:

> **Q6:** Information on whether, and if so how, the ASPSP has engaged with PISPs, AISPs and CBPIIs in the design and testing of the dedicated interface.

Testing

17.156 As set out in EBA Guidelines 6.4 and 6.5, ASPSPs that wish to be exempt need to have technical specifications and testing facilities available to AISPs, PISPs and CBPIIs no later than 14 March 2019 to qualify for an exemption. EBA Guideline 6.5 sets out the 7 areas (a-g) of connection and functional testing that need to be available in the testing facility.

17.157 The purpose of testing facilities is to allow AISPs, PISPs and CBPIIs, including AISPs and PISPs that are not yet authorised but are seeking authorisation, to undertake connection and functional testing of their software and applications used for offering a payment service to customers. Facilities should allow AISPs, PISPs and CBPIIs to test their software and applications before they launch their products to customers. Not all payment account products need to be reachable through the testing facility to meet the testing criteria.

17.158 In order to assess whether an ASPSP's dedicated interface meets the criteria set out in EBA Guideline 6, we require the following information:

> **Q7:** The date from which the ASPSP has made available, at no charge, upon request, the documentation of the technical specification of any of the interfaces specifying a set of routines, protocols, and tools needed by AISPs, PISPs and CBPIIs to interoperate with the systems of the ASPSP.

70 While OBIE was established under an order of the Competition and Markets Authority, other similar market initiatives exist, such as the Berlin Group in Germany https://www.berlin-group.org/psd2-access-to-bank-accounts

Q8: The date on which the ASPSP published a summary of the dedicated interface on its website. An ASPSP will need to provide a web link (URL) to the webpage where the technical specifications are provided. The published technical specifications must meet the requirements of SCA-RTS Article 30(3).

Q9: The date on which the testing facility became available for use by AISPs, PISPs and CBPIIs to test the dedicated interface in relation to points a-g in Guideline 6.5.

Q10: The number of different PISPs, CBPIIs, AISPs that have used the testing facility.

Q11: A summary of the results of the testing that has been undertaken using the available testing facilities. We do not need the results of testing with individual AISPs, PISPs and CBPIIs.

17.159 However, the summary of testing results should include:

- a summary of the feedback received from PISPs, AISPs and CBPIIs
- a summary of any issues identified
- a description of how any problems or issues have been addressed

17.160 Not all testing needs to have been completed by the time we receive the exemption request, as long as the available testing facilities meet Guideline 6.5 and Article 33(6)(b) of the SCA-RTS.

Testing certificates (EBA Guideline 6.5(b))

17.161 Under EBA Guideline 6.5(b), ASPSPs must make facilities available that enable AISPs PISPs and CBPIIs to test the ability to exchange the relevant certificates referred to in Article 34 of the SCA-RTS. In our view, prior to 14 September 2019, when certificates must comply with Article 34 of the SCA-RTS, where an authorised or registered AISP, PISP or CBPII does not yet have the relevant qualified certificate, this should not prevent them from making use of the testing facility.

Testing authentication procedures (EBA Guideline 6.5(g))

17.162 Under EBA Guideline 6.5(g), the ASPSP's testing facility must enable AISPs and PISPs to rely on all the authentication procedures provided by the ASPSP to its customers. Where an ASPSP is developing its authentication processes in order to meet strong customer authentication requirements by 14 September 2019, we acknowledge that this SCA functionality may not be fully ready for testing by March 2019. However, the testing facility should enable AISPs and PISPs to test the planned strong customer authentication scenarios so that they can be accommodated in their software and applications.

17.163 Under EBA Guideline 6.7, when assessing whether the dedicated interface has been designed and tested to the satisfaction of PSPs, we may take into account any problems reported to us by PISPs, AISPs and CBPIIs.

Wide usage of the interface (EBA Guideline 7)

17.164 Under SCA-RTS Article 33(6)(c), in order to exempt an ASPSP's dedicated interface, we must be satisfied that it has been widely used for at least 3 months by PSPs to offer account information services, payment initiation services and to provide confirmation on the availability of funds for card-based payments.

17.165 As per EBA Guideline 7.1, in order to assess whether this requirement is met, we will require an ASPSP to provide the following information:

> **Q12:** A description of the usage of the dedicated interface in a three-month (or longer) period prior to submission of the exemption request.

17.166 This description should include, but is not limited to providing: the number of PISPs, AISPs and CBPIIs that have used the interface to provide services to customers; and the number of requests sent by those PISPs, AISPs and CBPIIs to the ASPSP via the dedicated interface that have been replied to by the ASPSP.

17.167 The EBA has acknowledged that not all ASPSPs will be able to demonstrate wide usage of their dedicated interfaces in the run up to 14 September 2019. In our view, ASPSPs should aim to have the main interface functionality, which is likely to be subject to the most demand, in use before seeking an exemption. An explanation of which functionality has been in use should be provided in Q12 (for example 'AIS access to current account and credit card information has been in use since X date').

17.168 We also note that the results of some conformance testing can help to demonstrate that an ASPSP's dedicated interface is ready for use, where the ASPSP has not been able to demonstrate usage of aspects of the interface by AISPs, PISPs and CBPIIs.

17.169 The ASPSP must also provide evidence that it has made all reasonable efforts to ensure wide usage of the dedicated interface. In order to assess whether this is the case, in line with EBA Guideline 7.2(b), an ASPSP should provide the following information:

> **Q13:** A description of the measures undertaken to ensure wide usage of the dedicated interface, including by communicating its availability via appropriate channels, including where relevant the website of the ASPSP, social media, industry trade bodies, conferences and direct engagement with known market actors.

17.170 As per EBA Guideline 7.3, the three-month period referred to in letter (c) of Article 33(6) of the SCA-RTS may run concurrently with the testing referred to in Article 30(5) of the SCA-RTS. This means that where the ASPSP is meeting its requirement to allow testing from 14 March 2019, it may also meet its requirement to demonstrate wide usage of the interface for three months within this period.

Resolution of problems (EBA Guideline 8)

17.171 As per EBA Guideline 8, in order to exempt an ASPSP, we will need evidence that an ASPSP has systems and processes in place to resolve problems without undue delay (as required by SCA-RTS Article 33(6)(d)). An ASPSP should provide the following information, as per EBA Guideline 8.1:

Q14: Information on the systems or procedures in place for tracking, resolving and closing problems, particularly those reported by PISPs, AISPs and CBPIIs.

Q15: An explanation of the problems, particularly those reported by PISPs, AISPs and CBPIIs, that have not been resolved in accordance with the service level targets set out in Guideline 2.1.

17.172 ASPSPs should include a description of problems reported during both testing and operational use ('production') of the dedicated interface. We will take into account, as part of our assessment, problems reported by AISPs, PISPs and CBPIIs.

Revoking exemptions

17.173 Under SCA-RTS Article 33(7) the FCA is required to revoke an exemption where the conditions (a) and (d) of SCA-RTS Article 33(6) are not met by the ASPSP for more than 2 consecutive calendar weeks. Following an exemption being revoked, we are required to ensure that the ASPSP establishes, within the shortest possible time and at the latest within 2 months, the contingency mechanism referred to in SCA-RTS Article 33(4).

17.174 As noted in section 17.101, where the contingency mechanism is relied upon the ASPSP must ensure the customer's online banking portal meets the requirements of SCA-RTS Article 33. This includes providing a means for the AISP, PISP or CBPII to be identified and ensuring the AISP or PISP can rely on the authentication procedures provided by the ASPSP to the customer.

17.175 Reliance on the contingency mechanism should be a temporary measure. Where an exemption is revoked, we will expect the ASPSP to work towards providing access either:

- via the modified customer interface, which, in addition to general obligations for access interfaces, must also comply with SCA-RTS Articles 34 (certificates), 35 (security of communication session) and 36 (data exchanges), or
- via the dedicated interface which meets conditions (a) and (d) of SCA-RTS Article 33(6).

Reporting problems with the dedicated interface

17.176 SCA-RTS Article 33(3) requires ASPSPs, AISPs, PISPs and CBPIIs to report problems with the dedicated interface to their respective national competent authorities without undue delay. These problems are, as described in SCA-RTS Article 33(1):

i. The interface does not comply with requirements in SCA-RTS Article 32

ii. There is unplanned unavailability of the interface or a systems breakdown.

17.177 We will use the report required under SCA-RTS Article 33(3) as part of our monitoring of whether ASPSPs are complying with their obligations in respect of the interfaces that they put in place, in line with Article 30(6).

17.178 Where ASPSPs have been granted an exemption under SCA-RTS Article 33(5), we will also use the report to inform a decision whether it is appropriate to revoke the exemption. Under SCA-RTS Article 33(7) we are required to revoke an exemption from the contingency mechanism granted under SCA-RTS Article 33(6) where, for more than 2 consecutive calendar weeks, either:

- an ASPSP fails to comply with all the obligations in SCA-RTS Article 32, or
- problems related to the dedicated interface have not been resolved without undue delay.

17.179 Problems with dedicated interfaces should also be separately assessed against the criteria in the EBA Guidelines on major incident reporting under PSD2 to determine whether they qualify as a major incident (see **Chapter 13 – Reporting and notifications**).

How to report

17.180 Details of how to report using Form NOT005 can be found in Chapter 13 and SUP 15.14.38

What to report

17.181 The reporting form will allow a reporting ASPSP, AISP, PISP or CBPII to select which of the two categories its report is about. The following sections provide detail about the information to provide for each category.

i. Article 32 requirements

17.182 Where an ASPSP, AISP, PISP or CBPII believes that an ASPSP's interface is not performing in compliance with SCA-RTS Article 32, it must submit report using Form NOT005 (available via Connect) and include a short summary of the reasons it believes SCA-RTS Article 32 requirements are not being met. A non-exhaustive list of reasons that could be given include:

- The uptime of the dedicated interface as measured by the KPIs described in EBA Guidelines 2.2 and 2.4, falls below the uptime of the interface used by the ASPSP's customers.
- There is not the same level of support offered to AISPs, PISPs and CBPIIs using the ASPSP's dedicated interface, in comparison to the customer interface. In our view, support could include, for example, service desks, or hotlines to deal with issues.
- The dedicated interface poses obstacles to the provision of payment initiation and account information services (see SCA-RTS Article 32 and the EBA Guidelines and Opinion).

ii. Unplanned unavailability of the interface or a systems breakdown

17.183 Under SCA-RTS Article 33(1), unplanned unavailability or a systems breakdown may be presumed to have arisen when five consecutive requests for access to information for the provision of payment initiation services or account information services are not replied to within 30 seconds. The FCA encourages AISPs, PISPs and CBPIIs to submit a report concerning unplanned availability or systems breakdown only after this threshold has been passed in respect of requests made by that AISP or PISP.

17.184 PISPs and CBPIIs can also use the form to report that the ASPSP has failed to provide to the CBPII or to the PISP a 'yes' or 'no' confirmation in accordance with article 65(3) of PSD2 and article 36(1)(c) of the RTS.

17.185 The information that a PISP can request (and an ASPSP must provide) is set out in regulation 69(2)(b) of the PSRs 2017 and SCA-RTS Article 36(1)(b) and (c). Treatment of data requests by AISPs is set out in regulation 70(2)(b) of the PSRs 2017 and SCA-RTS Article 36(1)(a). These provisions should be read in conjunction with our guidance in sections 17.29-30 and 17.33 of this chapter. The FCA will not act on reports describing a failure of an ASPSP to provide information that the ASPSP is not obliged to provide.

17.186 We agree with the EBA's Opinion that an ASPSP is obliged to provide immediate confirmation, in a 'yes' or 'no' format, of whether there are funds available at the request of a PISP under SCA-RTS Article 31(1)(c). PISPs are not generally entitled to know the balance of funds or transaction history in order to manage execution risk. However, where an ASPSP's system does not enable it to provide such a 'yes' or 'no' answer, the ASPSP should give PISPs the possibility of accessing any data that the ASPSP uses to determine whether or not to execute a customer payment, for instance any incoming/outgoing payments that will affect the balance or overdraft (see section 17.26).

17.187 Where the ASPSP does not provide such a 'yes' or 'no' answer and after five consecutive requests does not provide the information required for a PISP to manage execution risk, the PISP can report under Article 33(1) using the 'other unplanned unavailability or systems breakdown' option in NOT005, and providing a brief description.

17.188 The report will ask an AISP, PISP, CBPII or ASPSP to confirm that the report is in relation to unplanned availability or systems breakdown and to provide a brief description. Examples of the brief descriptions an AISP, PISP or ASPSP can select include:

- Unavailability after 5 consecutive requests of information on the initiation of the payment transaction and all information accessible to the ASPSP regarding the execution of the payment transaction.
- Unavailability after 5 consecutive requests of information from designated payment accounts and associated payment transactions made available to the customer when directly requesting access to the account information excluding sensitive payments data.[71]
- Failure to provide to the card based payment instrument issuer (CBPII) or to the PISP a 'yes/no' confirmation in accordance with article 65(3) of PSD2 and article 36(1)(c) of the RTS.
- Other unplanned unavailability or systems breakdown.

17.189 The reporting AISP, PISP, CBPII or ASPSP should also confirm using the specified part of the form whether availability has been restored at the time of reporting.

71 See section 17.62 for more guidance on sensitive payments data

18 Operational and security risks

Introduction

18.1 All PSPs are required by ~~Regulation~~regulation 98 of the PSRs 2017 to establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks relating to the payment services they provide. As part of that framework they must establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents.

18.2 All PSPs must provide the FCA, on at least an annual basis, with an updated and comprehensive assessment of the operational and security risks relating to the payment services they provide. This must include an assessment of the adequacy of the mitigation measures and control mechanisms implemented in response to those risks. **Chapter 13 – Reporting and notifications** contains more information.

18.3 In accordance with SUP16.13.12, PSPs are directed to comply with the European Banking Authority Guidelines on security measures for operational and security risks of payment services under PSD2 (the EBA Guidelines), as issued on 12 December 2017.[~~53~~72]

18.4 This chapter does not give guidance on specific provisions, or the application, of the EBA Guidelines. Rather, it explains some of the factors that we expect PSPs to take into account when developing, reviewing or maintaining their operational and security risk management framework. This guidance must be read alongside the EBA Guidelines.

18.5 This chapter is relevant to all PSPs. FSMA authorised firms should also comply with relevant provisions of the Senior Management Arrangements, Systems and Controls (SYSC) module of the FCA Handbook.

18.6 A PSP's approach to operational and security risk management should be proportionate to its size and the nature, scope, complexity and riskiness of its operating model, and of the payment services it offers. The FCA will supervise PSPs in accordance with its general approach to supervision.

Agents

18.7 As part of identifying operational and security risks, PSPs should consider how the use of agents introduces operational or security risks. Whenever a PSP has asked another party to carry out a payment service on its behalf, we would expect the PSP to have considered where any operational and security risk might lie when complying with its obligations under the Guidelines. For example, in establishing its risk management

~~53~~72 European Banking Authority Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2) (12 December 2017) http://www.eba.europa.eu/-/eba-publishes-final-guidelines-on-security-~~measures-under-psd2~~measures-under-psd2

framework and establishing and implementing preventive security measures (as set out in Guidelines 2 and 4 of the EBA Guidelines).

18.8 In these circumstances, it is the responsibility of the PSP to ensure that all identified risks including those arising from, or related to, agents are mitigated. Regulated firms retain full responsibility and accountability for discharging all their regulatory responsibilities, even when certain activities are carried out by third parties. We remind PSPs of their obligations under ~~Regulations~~regulations 6, 34 and 37 of the PSRs 2017 and under other relevant EBA Guidelines (e.g. the EBA Guidelines on Authorisation and Registration under PSD2).

Outsourcing

18.9 **Chapter 4 – Changes in circumstances of authorisation or registration** provides more information about requirements when PSPs intend to enter into outsourcing contracts if they will be relying on a third party to provide an operational function relating to the provision of payment services or electronic money services ("outsourcing").[~~54~~73]

18.10 Where a PSP outsources functions relevant to the payment services it offers, its operational and security risk framework should set out mitigation measures or controls to account for any operational and security risks identified from the outsourcing of those functions. These risks may arise from the relationship between a PSP and the party offering outsourced services, or they may relate to how the PSP monitors risks relating to these activities. The PSP should demonstrate that it has monitored and sought assurance on the compliance of outsourcers with security objectives, measures and performance targets.

18.11 Where relevant, PSPs must also consider requirements under FSMA, the FCA Handbook (especially SYSC 8) and other regimes. Any PSP wishing to outsource activities to the cloud or other third-party IT services should consider the FCA's guidance in FG16/5.[~~55~~74]

18.12 Although outsourced service providers may not fall within the FCA's regulatory perimeter, all PSPs should bear in mind that they retain full responsibility and accountability for discharging all of their regulatory responsibilities. They must comply with the obligations set out in ~~Regulation~~regulation 25 of the PSRs 2017. This includes where

an AIS or PIS provider makes use of other businesses to access and/or consolidate payment account information.

18.13 Firms cannot delegate their regulatory responsibility or their responsibility to their payment service users to another party. A relevant act or omission by another party to which a PSP has outsourced activities will be considered an act or omission by the PSP. Any outsourcing will be a relevant consideration in the context of risk assessments, required under Guideline 3 of the EBA Guidelines.

5473 See specifically 4.54 to 4.58 of Chapter 4 – Changes in circumstances of authorisation or registration.

5574 Finalised Guidance FG 16/5 'Guidance for firms outsourcing to the 'cloud' and other third-party IT services' (July 2016). Available at https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf

Risk assessments

18.14 Guideline 3 of the EBA Guidelines sets out the requirements on PSPs when undertaking risk assessments. PSPs should take into account all the factors that could affect the risk assessments they carry out. For example, we would expect an AIS or PIS provider to assess and identify risks related to the method that is used to access payment accounts, and to demonstrate how they mitigate any identified risks. Consequently, where an AIS or PIS provider does not access payment accounts through dedicated interfaces, for example, by accessing payment accounts directly itself or by using a third party, we would expect the risk assessment to demonstrate how the provider mitigates any identified risks related to its method of access.

18.15 PSPs are reminded that they must comply with all relevant data protection law, ~~SYSC[56]~~ SYSC[75] and other systems and control requirements. More information is available in **Chapter 17 – Payment initiation and account information services and confirmation of availability of funds**.[~~57~~76]

18.16 PSPs that choose not to apply strong customer authentication under Article 17 of Commission Delegated Regulation (EU) 2018/389[77] (the SCA-RTS) must address the corporate payment processes and protocols not subject to strong customer authentication in the risk assessment, which should include a brief description of the payment service and how equivalent levels of security have been achieved. Firms intending to operate under this exemption will need to ensure that they have provided us with this information by including it in an assessment submitted at least 3 months in advance of the date of intended use. **Chapter 20 – Authentication** (section 20.57 – 20.63) provides further information.

Best practice standards

18.~~16~~17 PSPs should review our joint statement with HM Treasury on third party access provisions in PSD2.[~~58~~78] We are also aware of industry initiatives to develop standards on access to accounts before the RTS on SCA and CSC come into force. PSPs may wish to take account of best practice standards, where relevant.[~~59~~79]

~~56~~75 https://www.handbook.fca.org.uk/handbook/SYSC/

~~57~~76 See from 17.51 to 17.59

~~58~~77 The SCA-RTS is available here https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN

78 See our joint statement with HMT 'Expectations for the third party access provisions in Payment Services Directive II' (July 2017) available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/630135/Expectations_for_the_third_party_access_provisions_in_PSDII.pdf

~~59~~79 For example, the voluntary guidelines published jointly by UK Finance, the Financial Data and Technology Association (FDATA), the Electronic Money Association (EMA) and techUK "Voluntary guidelines and encouraged market behaviours under PSD2 in the 'transitional period'" available at https://www.ukfinance.org.uk/wp-content/uploads/2018/01/Voluntary-Guidelines-and-Encouraged-Market-Behaviours-Under-PSD2-FINAL.pdf (14 May 2018).

19 Financial crime

~~**Note: This chapter references regulatory technical standards (RTS) yet to be finalised at time of publication. It will be updated, where necessary, once these instruments are finalised.**~~

Introduction

19.1 All payment service providers (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~~[60] Regulation[80]
- section 21A of the Terrorism Act 2000
- the Proceeds of Crime Act 2002
- the relevant financial crime provisions of the Payment Services Regulations 2017 (PSRs 2017) and Electronic Money Regulations 2011 (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.[61] [81]

19.4 Credit institutions that provide payment services or issue e-money are subject to additional 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.

Financial crime and passporting

19.5 Authorised payment institutions (PIs), authorised e-money institutions (EMIs) and registered account information service providers (RAISPs) who wish to provide payment services (or, in the case of authorised EMIs, distribute or redeem e-money)

~~60 EU Regulation 847/2015 makes changes to the rules on wire transfers previously set out in EU Regulation 1781/2006.~~

~~61 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.~~

through an establishment in another European Economic Area (EEA) State in accordance with **Chapter 6 – Passporting**, must comply with the relevant anti-money laundering and counter terrorist financing laws enacted in that EEA State. Firms should check what their obligations will be in the host state and take steps to comply with that-

80 EU Regulation 847/2015 makes changes to the rules on wire transfers previously set out in EU Regulation 1781/2006.

81 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.

law. Where the firm's head or registered office is in the UK, under the MLRs the branch will be deemed to be carrying on business in the UK and will be subject to the MLRs as well as the host state's money laundering regime.

19.6 In certain circumstances host states may require, under Regulatory Technical Standards developed by the European Banking Authority (EBA) under the fourth Money Laundering Directive, the appointment of a central contact point in the host state for anti-money laundering and counter terrorist financing purposes.[62] PSD2 also contains separate provisions relating to the power of host states to require the appointment of a central contact point for supervisory purposes where a PI, EMI or RAISP 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, EMIs and RAISPs.

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 We have 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 Under the MLRs, PSPs and e-money issuers are required to demonstrate that they establish and maintain policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing. Appropriate policies and procedures are proportionate to the nature, scale and complexity of the PSP's

62 EBA 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 26 June 2017, available here: https://www.eba.europa.eu/-/esas-publish-central-contact-point-standards-in-fight-against-financial-crime. These RTS will not come into force until published in the EU's Official Journal, after which they will become a Commission Delegated Regulation.

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, a PSP or e-money issuer should consider a range of factors, including (where they are relevant):

82 'Commission Delegated Regulation (EU) 2018/1108 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council with regulatory technical standards on the criteria for the appointment of central contact points for electronic money issuers and payment service providers and with rules on their functions' is available here: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1108&from=EN

- its customer, product and activity profiles;
- its distribution channels;
- the type, complexity and volume of permitted transactions;
- 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 money laundering or terrorist financing purposes, we expect PSPs and e-money issuers 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 PSPs and e-money issuers 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. PSPs and e-money issuers 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 the sale of age-restricted goods to minors.

19.14 PSPs and e-money issuers should carry out regular assessments of their anti- money laundering policies and procedures to ensure that they remain relevant and appropriate. As part of this, PSPs and e-money issuers should be alert to any change in their operating environment that will have an impact on the way that they conduct their business. For example, we expect PSPs and e-money issuers 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 into their risk assessment as appropriate.

Agents, branches and outsourced providers

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, agents (and distributors in the case of EMIs), branches or outsourced providers to the same extent as if they have expressly permitted it. This includes a failure to take adequate measures to prevent money laundering and terrorist financing, as well as failure to comply with the UK's financial sanctions regime. 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.

Internal organisation

19.17 We expect PSPs and e-money issuers 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.

19.18 Regulation 21(1)(a) of the MLRs requires PSPs and e-money issuers (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) of the MLRs specifically requires PSPs and e-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 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 PSP or e-money issuer and sufficient access to resources and information to enable him/her to carry out that responsibility.

Industry guidance

19.19 When considering whether a breach of applicable legislation in relation to anti-money laundering and counter-terrorist financing has occurred in relation to a firm that we supervise for anti-money laundering purposes, we will consider whether a PSP or e-money issuer has followed relevant provisions in the guidance for the UK financial sector issued by the Joint Money Laundering Steering Group (JMLSG). PSPs are reminded that the JMLSG does not intend its guidance to be applied without thought, as a checklist of steps to take. PSPs and e-money issuers should also have regard to our guidance on the treatment of politically exposed persons (PEPs) when meeting their anti-money laundering obligations.[~~63~~83]

Communications with customers

19.20 A PSP's legal and regulatory obligations to communicate with customers and third parties will not constitute 'tipping off' under section 333A of the Proceeds of Crime Act 2002) unless:

- the PSP or another person has made a lawful disclosure (e.g. a Suspicious Activity Report made to the National Crime Agency); or
- the PSP or another person discloses that an investigation into allegations that an offence relating to money laundering is being contemplated or is being carried out;

and the relevant communication is likely to prejudice any investigation that might be conducted following the disclosure.

~~63~~

83 https://www.fca.org.uk/publication/finalised-guidance/fg17-06.pdf

Enforcement

19.21 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 fails to meet its obligation to put in place effective procedures in relation to financial crime.

19.22 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 other financial crime obligations under other legislation, including the Financial Services and Markets Act 2000, the MLRs and Schedule 7 to the Counter-Terrorism Act 2008.

19.23 See **Chapter 14 – Enforcement** for more details about our enforcement approach.

20 Authentication

20.1 This chapter describes the authentication and security measures that apply to all payment service providers (PSPs) subject to the PSRs 2017 – including e-money institutions when providing payment services and registered account information service providers (RAISPs).

20.2 Although exempt from the PSRs 2017, credit unions should also consider reading this chapter. Under BCOBS 5.1.10A, these firms must consider the risk of fraud and put in place appropriate procedures and technical safeguards to ensure that such payments can be carried out in a safe and secure manner. As part of this, such firms may wish to consider the adoption of 'strong customer authentication' as specified in the Regulatory Technical Standards on strong customer authentication and common and secure communication[84] (the 'SCA-RTS') and discussed in this chapter.

20.3 Authentication is a procedure which allows a PSP to verify the identity of a payment service user or the validity of the use of a specific payment instrument. The purpose is to ensure that the payment service user is the legitimate user and has given their consent for the transfer of funds or access to their account information.

20.4 From 14 September 2019, all PSPs must comply with regulation 100 of the PSRs 2017 and with the SCA-RTS published in the form of a Commission Delegated Regulation. The European Banking Authority (EBA) has published an Opinion[85] on the implementation of the SCA-RTS (the 'EBA Opinion') to provide additional clarity on certain aspects of the requirements.

20.5 The SCA-RTS specifies:

- requirements for PSPs to put in place transaction monitoring mechanisms and to conduct regular security reviews
- requirements for the application of strong customer authentication
- conditions where exemptions from strong customer authentication may be applied
- requirements to protect the confidentiality and integrity of the payment service user's personalised security credentials[86]
- requirements for common and secure open standards of communication.

84 The Commission Delegated Regulation (EU) 2018/389 (the SCA-RTS) is available here https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN

85 The EBA Opinion is available here: https://www.eba.europa.eu/documents/10180/2137845/Opinion+on+the+implementation+of+the+RTS+on+SCA+and+CSC+%28EBA-2018-Op-04%29.pdf/0f525dc7-0f97-4be7-9ad7-800723365b8e

86 Personalised security credentials are personalised features provided by a PSP to a payment service user for the purposes of

authentication as defined in regulation 2 of the PSRs 2017.

General provisions

20.6 All PSPs are required to establish transaction monitoring mechanisms (specified in SCA-RTS Article 2) to enable them to detect unauthorised or fraudulent payment transactions. While not required, we encourage PSPs to consider adopting a real-time risk analysis approach on a similar basis to that described in SCA-RTS Article 18(2)(c) for the purpose of meeting the requirement of SCA-RTS Article 2.

20.7 As stated in SCA-RTS Article 3, PSPs are required to document, periodically test, evaluate and audit the security measures implemented in compliance with the SCA-RTS. Firms should be prepared to provide us with such evaluation and audit reports upon our request. A payment institution's or e-money 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 contravention of any requirements imposed by or under the PSRs 2017 or Electronic Money Regulations (EMRs) that is of material significance to us (regulation 25 of the EMRs and regulation 24 of the PSRs 2017). Banks and building societies, and their auditors, are subject to different audit requirements under SUP 3 of the FCA Handbook.

Strong customer authentication

20.8 Regulation 100(1) of the PSRs 2017 states that a PSP must apply strong customer authentication where a payment service user:

- accesses their payment account online, whether directly or through an account information service provider
- initiates an electronic payment transaction, or
- carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

20.9 The requirements for strong customer authentication apply to all electronic payment transactions initiated by the payer and to card payment transactions initiated through the payee. They also apply regardless of whether the payment service user is a consumer or a business.

20.10 In line with the EBA Opinion (paragraph 36), strong customer authentication is required both to access payment account information and to initiate a payment transaction. Where a payment service user wishes to initiate a payment within a session in which strong customer authentication was performed to access online data, application of strong customer authentication will be required again for the payment initiation, unless the ASPSP chooses to apply one of the exemptions permitted under regulation 100(5) of the PSRs 2017.

20.11 SCA-RTS Recital 8 clarifies that payments made through the use of anonymous payment instruments (such as certain pre-paid gift cards) are not subject to the obligation of strong customer authentication. In our view, in line with Recital 95 of PSD2, telephone banking (eg where customers contact their bank to check their balance or to pay their credit card bill over the phone), paper-based payment transactions (including written instructions given by a customer to set up a series of

recurring payments), mail orders and telephone orders are out of scope of regulation 100 of the PSRs 2017. Nonetheless, we expect firms to put in place procedures and safeguards to protect customers using such channels from the risk of fraud. PSPs may wish to consider extending the authentication requirements to these channels on a voluntary basis. In addition, PSPs may be subject to other requirements to combat fraud and financial crime under legislation, including FSMA, the Money Laundering, Terrorist Financing and Transfer of Funds (Information to the payer) Regulations 2017 (MLRs) and the FCA Handbook.

20.12 Regulation 63 of the PSRs 2017 defines the territorial scope of regulation 100 of the PSRs 2017. As acknowledged in EBA Opinion paragraph 32, in the case of cross-border transactions where only the payer's PSP or the payee's PSP is located within the EEA, there may be limitations on the extent to which the requirements can be applied beyond a 'best efforts' basis. For example, where a UK cardholder makes a purchase with a merchant whose PSP (card acquirer) is located in a jurisdiction not legally subject to PSD2, the UK PSP (card issuer) should make every reasonable effort to determine the legitimate use of the payment instrument.

20.13 SCA-RTS Articles 4 to 9 specify the security requirements for strong customer authentication. In accordance with regulation 100(3) of the PSRs 2017 and SCA-RTS Articles 22 to 27, PSPs must maintain adequate security measures to protect the confidentiality and integrity of payment service users' personalised security credentials.

Use of multiple authentication factors

20.14 Strong customer authentication is intended to enhance the security of payments. It enables a PSP to have greater certainty that a payment service user wishing to make a payment, or to access their account, is a legitimate payment service user and not a fraudster.

20.15 Under the PSRs 2017, strong customer authentication[87] means authentication based on the use of two or more independent elements (factors) from the following categories:

- something known only to the payment service user (knowledge)
- something held only by the payment service user (possession)
- something inherent to the payment service user (inherence[88]).

20.16 When designing the authentication method, the PSP must ensure the factors are independent (SCA-RTS Article 9). Therefore, the breach of one factor should not compromise the reliability of any other factor, and the confidentiality of the authentication data should be protected.

20.17 Independent factors may be hosted on the same device. However, where any of the factors or the authentication code itself is used through a multi-purpose device (such

87 Strong customer authentication is defined in regulation 2 of the PSRs 2017

88 An example of inherence is a biometric characteristic such as an iris scan or fingerprint but can also include behavioural biometrics, provided they comply with the requirements under SCA-RTS Article 8.

as a tablet or mobile phone, which can be used to initiate the transaction and can play a role in the authentication process), PSPs must adopt security measures to mitigate against the risk of compromise of that device. SCA-RTS Articles 6, 7 and 8 set out the requirements the factors from each category must meet.

20.18 For any application of strong customer authentication, as a minimum the factors used must derive from at least two out of the three categories. For example, a password (knowledge) and a fingerprint (inherence) would meet the requirements but a password and a personal identification number (PIN) would not, as both are knowledge factors. Where certain static information is displayed on a payment card, such as the card verif ication number (CVV), the long, primary account number (PAN) and the expiry date, it cannot be used as a knowledge factor. It may however be used as evidence of the possession of a card (subject to the requirements in SCA-RTS Article 7), alongside use of a knowledge factor (such as a static password or one-time password) or an inherence factor (such as a finger print or behaviour-based biometric credentials). Use of a dynamic CVV (where a CVV code is displayed electronically on a payment instrument and changes periodically) is stronger evidence of possession of a payment card, as it prevents card details being used in the absence of the physical payment card itself. Use of a card reader can also validate that a payment card is in the possession of the legitimate payment service user.

20.19 For use of a device (such as a mobile phone) to be considered as possession, there needs to be a reliable means to confirm the device is in the payment service user's possession through the generation or receipt of a dynamic validation element on the device. This could include, but is not limited to, use of a token generator, or receipt of a one-time password sent via SMS which can be used to validate possession of the SIM-card associated with the customer's mobile phone number (provided that its use is 'subject to measures designed to prevent replication of the elements' as required under SCA-RTS Article 7(2)).

20.20 Biometric credentials associated with the payment service user can be used as inherence factors, even when hosted at device level (eg using fingerprint authentication on a mobile phone), provided appropriate risk-mitigation measures have been taken to link the device securely to the customer.

20.21 We encourage firms to consider the impact of strong customer authentication solutions on different groups of customers, in particular those with protected characteristics, as part of the design process. Additionally, it may be necessary for a PSP to provide different methods of authentication, to comply with their obligation to apply strong customer authentication in line with regulation 100 of the PSRs 2017. For example, not all payment service users will possess a mobile phone or smart phone and payments may be made in areas without mobile phone reception. PSPs must provide a viable means to strongly authenticate customers in these situations.

Application of strong customer authentication in the context of payment initiation services and account information services

20.22 Under regulation 100(4) of the PSRs 2017, an account servicing payment service provider (ASPSP) must allow a payment initiation service provider (PISP) or an account information service provider (AISP) to rely on the authentication procedures provided by the ASPSP to the payment service user.

20.23 Recital 30 of PSD2 clarifies that the personalised security credentials used for strong customer authentication are usually those issued by the ASPSP to the payment service user. Regulations 69(3)(b) and 70(3)(b) require a PISP or an AISP to ensure that the credentials are not accessible to other parties (except the issuer of the credentials) and are transmitted securely. An AISP or PISP can still rely on the credentials issued by the ASPSP if the AISP or PISP's payment service user is redirected to the ASPSP for the purpose of authentication (see section 17.133 on redirection).

20.24 As noted in the EBA Opinion, it is possible for a PISP and an AISP to issue their own credentials to be used by the payment service user to access the PISP's or AISP's own platform (such as an application or website). However, only the credentials issued by the ASPSP can be used to meet the requirement for strong customer authentication. It is open to the ASPSP to allow a PISP, an AISP or another party (such as a merchant or mobile wallet provider) to apply strong customer authentication on the ASPSP's behalf as part of a bilateral contract or arrangement. We would expect the parties to ensure that the contract addresses the allocation of liability between the parties.

20.25 When initiating a payment using a PISP, a payment service user might need to select the account within the ASPSP's domain. The ASPSP may show the account balances as part of this. In our view, strong customer authentication need only be applied once in this payment initiation process.

Authentication code

20.26 In accordance with SCA-RTS Article 4, application of strong customer authentication based on two or more authentication factors must generate an authentication code. The SCA-RTS does not specify how to implement the authentication code. However, SCA-RTS Recital 4 refers to authentication codes based on solutions such as generating and validating one-time passwords, digital signatures or other cryptographically underpinned validity assertions using keys or cryptographic material stored in the authentication elements, provided the security requirements are met.

20.27 The authentication code must only be accepted once by the PSP in relation to the payer accessing its payment account online, initiating an electronic transaction or carrying out any action through a remote channel which may imply a risk of payment fraud or other abuses. There is no specific requirement for the authentication code to be visible to the payment service user or for the payment service user to input it themselves. However, it must meet the requirements detailed in SCA-RTS Article 4.

20.28 In line with SCA-RTS Article 4(2), PSPs must ensure that:

- no information about any of the factors can be derived from disclosure of the authentication code
- knowledge of previously generated codes cannot enable a new authentication code to be generated
- the authentication code cannot be forged

20.29 In line with SCA-RTS Article 4(3)(a), PSPs must ensure that where authentication fails to generate an authentication code, it shall not be possible to identify which of the

authentication factors was incorrect. This means that any failure message should not disclose which authentication element was incorrect. However, this does not prevent a PSP from prompting a customer to re-attempt or re-start the authentication process.

20.30 In accordance with regulation 100(3) of the PSRs 2017 and SCA-RTS Article 22, PSPs must maintain adequate security measures to protect the confidentiality and integrity of payment service users' personalised security credentials. This includes protection of authentication codes during all phases of the authentication.

20.31 Under SCA-RTS Article 4(3)(b), the number of consecutive failed authentication attempts is limited to no more than five within a given period of time. In the FCA's view, a failed authentication attempt could include instances where the PSP does not recognise the authentication code provided to be valid, or to match the code that was generated. Where there are five consecutive failed attempts, the PSP must block the relevant action (i.e. the customer's access to the payment account or initiation of an electronic payment transaction). Where the block is temporary, the duration should be in accordance with SCA-RTS Article 4(4). Where the block is permanent, the payment service user must be notified in advance of the block and a secure procedure must be established to allow the payer to regain use of the blocked electronic payment instruments (eg. a secure procedure for being sent a new payment card).

20.32 In addition, SCA-RTS Article 4(3)(d) states that the maximum time without activity of the payer after authentication shall not exceed 5 minutes. In our view, this means that a payment service user, after successfully authenticating to access their payment account, should no longer have access to the payment account after no more than 5 minutes of inactivity has elapsed. If a payment service user wishes to access its account again, the PSP must perform strong customer authentication unless one of the exemptions is available. This requirement only applies to scenarios where strong customer authentication was applied by the PSP. Where strong customer authentication is not applied (eg because a PSP chooses to apply an exemption), we encourage PSPs to consider setting their own session inactivity rule as a security measure. We encourage firms to consider the impact of strong customer authentication solutions on different groups of customers, in particular those with protected characteristics, as part of the design process.

Dynamic linking

20.33 Regulation 100(2) of the PSRs 2017 and SCA-RTS Article 5 require that for electronic remote payment transactions, PSPs must apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee. In other words, PSPs must ensure the authentication code generated and accepted by the PSP is specific to an amount and to the identity of the payee (for example the payee's trading name) agreed to by the payer when initiating the transaction. Accordingly, any change to the amount or the payee's name must invalidate the authentication code generated in line with SCA-RTS Article 5(1)(d).

20.34 As described in Recital 95 of PSD2, the requirement applies to payment services offered via internet or other at-distance channels, the functioning of which does not depend on where the device used to initiate the payment transaction, or the payment instrument used, are physically located. Examples of an electronic remote payment include where a payment service user is transferring funds using online banking or a

mobile banking application, or making a purchase online via a merchant's website using a card-based payment or a payment initiation service. In our view, where payments can be initiated at an ATM, such payments do not qualify as remote and dynamic linking is not required.

20.35 In relation to remote card-based transactions initiated through a payee where the amount is not known in advance[89] (see section 8.225 – 8.229), the authentication code will still need to specify an amount that has been authorised by the payment service user.

20.36 The payee has the option to either charge the customer for the value of the goods or services at the time the order is placed, or obtain the customer's authorisation for a maximum amount at that time but charge the customer the final amount once it is known.

- If charging the customer at the time the order is placed, in the event the final amount is lower, the payee would refund the difference in accordance with its legal obligations. If the final amount is higher (eg due to substituted goods), the payee could obtain the payer's authorisation for a further payment (which would be subject to strong customer authentication unless an exemption applied).

- If charging the customer once the final amount is known, the payer's PSP (the card issuer) must re-apply strong customer authentication in the event that the actual amount is higher than the pre-authorised amount even if only incrementally, (unless an exemption is used). If the actual amount is lower than the pre-authorised amount, strong customer authentication would not need to be re-applied. When obtaining the customer's authorisation the merchant could optionally request the funds to be blocked. In this scenario, the authentication code is required to be specific to the exact amount that the payer has consented to be blocked, in accordance with regulation 78 of the PSRs 2017 and SCA-RTS Article 5(3)(a). If the merchant does not request an amount of funds to be blocked, the customer's authorisation must still be for a specific maximum amount.

20.37 Similarly, in cases where a payer gives consent to execute a batch of remote electronic payments to one or several payees, the authentication code must be specific to the total amount of the batch and the specified payees. For example, in the case of split shipments, the code should specify the total amount to cover multiple purchases from a merchant where the goods purchased are shipped, and related individual payments are taken, at different times. This also applies in the travel industry where an online travel agent obtains the customer's authorisation for the total value of an itinerary and there are multiple underlying travel provider payees (eg airline, hotel and excursions).

Exemptions from strong customer authentication

20.38 Regulation 100(5) of the PSRs 2017 refers to exemptions from strong customer authentication provided for in the SCA-RTS. These have been defined on the basis of the level of risk, amount, recurrence and the payment channel used for the execution

89 Examples include online grocery shopping where the customer may add items or the merchant may substitute items; hotel bills and car hire

of the payment transaction in accordance with Article 98(3) of PSD2. This section sets out our views on each exemption.

20.39 SCA-RTS Articles 10 to 18 specify the conditions under which the PSP is allowed not to apply strong customer authentication in relation to:

- access to payment account information (SCA-RTS Article 10)
- contactless payments at point of sale (SCA-RTS Article 11)
- unattended terminals for transport fares and parking fees (SCA-RTS Article 12)
- trusted beneficiaries (SCA-RTS Article 13)
- recurring transactions (SCA-RTS Article 14)
- credit transfers between accounts held by the same natural or legal person (SCA-RTS Article 15)
- low-value transactions (SCA-RTS Article 16)
- secure corporate payment processes and protocols (SCA-RTS Article 17)
- transaction risk analysis (SCA-RTS Article 18)

20.40 The payer's PSP (eg the ASPSP or card issuer) has the right to decide not to apply strong customer authentication where the conditions for exemption are met, in line with SCA-RTS Recital 17. Equally, the payer's PSP may choose not to use some or all of the exemptions and, instead, apply strong customer authentication for all transactions. PSPs that make use of any of the exemptions are permitted, at any time during the course of the action or payment transaction, to choose to apply strong customer authentication.

20.41 The exemptions are separate and independent from one another. Where a payment transaction may qualify for an exemption under several different categories (eg a low-value transaction at an unattended car park terminal) the PSP may choose which, if any, relevant exemption to apply. PSPs should note that for the purpose of reporting fraud under regulation 109 of the PSRs 2017 and the EBA Guidelines on fraud reporting, fraudulent transactions should be assigned to a specific exemption and reported under one exemption only.

20.42 Ultimately, it is the payer's PSP that decides whether or not to apply one of the permitted exemptions and not the payee's. In line with the EBA Opinion, in certain circumstances, in the context of card payment transactions, the payee's PSP (the card acquirer) may apply an exemption. It is our view, however, that even in such cases, the payer's PSP (the card issuer) retains the right to require strong customer authentication. Regulation 77(6) of the PSRs 2017 addresses the subject of liability in the event that the payee or the payee's PSP does not accept strong customer authentication (see 8.223). When deciding whether to require strong customer authentication or to apply an appropriate exemption, ASPSPs are reminded of their obligation to treat payment orders received from PISPs in the same way as a payment order received directly from the payer, unless the ASPSP has objective reasons for treating the payment order differently (see 17.31).

Payment account information (SCA-RTS Article 10)

20.43 Under SCA-RTS Article 10(1), the PSP may allow access to payment account information (the account balance or a list of payment transactions executed in the last 90 days or both) without requiring strong customer authentication. If the customer is accessing historical transaction information covering transactions executed over 90 days ago, strong customer authentication will be required.

20.44 SCA-RTS Article 10(2) states that the PSP cannot apply the exemption where either the customer is accessing the payment account information online for the first time or it is more than 90 days since the customer accessed the online information and strong customer authentication was applied.

20.45 The conditions for the SCA-RTS Article 10 exemption apply whether the customer is accessing the payment account information online directly or using an AISP. The EBA Opinion sets out that the 90-day period is specific to each AISP and needs to be distinguished from the 90-day period that applies to direct access by the customer. That is to say, a customer accessing their payment account directly will not reset the 90-day counter that applies when access to that same payment account is through a particular AISP.

20.46 The EBA Opinion also states that application of strong customer authentication for the purposes of payment initiation (directly by a payment service user or via a PISP) during this period does not restart the 90-day count. Consequently, it will be necessary to keep track of how many days have elapsed since an individual AISP accessed the payment service user's payment account using strong customer authentication. The EBA Opinion suggests that generation of a response code to indicate when the 90-day limit has been exceeded is an option.

20.47 The intention behind these provisions is to ensure that all AISPs need to ask customers to provide strong customer authentication periodically, in order to prompt customers to reassess whether they still wish to consent to their data being accessed. In our view there is no reason why the AISP and ASPSP cannot agree a process for this purpose (see 20.24). We strongly encourage firms and API initiatives to look for ways to facilitate and to streamline this process to minimise the impact on customers, AISPs and ASPSPs.

Contactless payments at point of sale and low-value transactions (SCA-RTS Articles 11 and 16)

20.48 In the context of contactless payments at point of sale (SCA-RTS Article 11) and low-value transactions (SCA-RTS Article 16), in addition to the monetary limit on the individual transaction, PSPs can apply either the cumulative monetary amount or the limit on the number of consecutive transactions but not both. It may be preferable for PSPs to decide which one of these measures to use in all cases to avoid confusing payment service users. We recognise that fluctuations in exchange rates between euro and sterling, in respect of the euro-denominated limits and thresholds in SCA-RTS Article 11 and Article 16, and in relation to Article 18 (transaction risk analysis), may cause operational difficulties and customer confusion. We expect PSPs to take a reasonable and consistent approach to dealing with such fluctuations. This may include use of rounding to a sensible sterling amount, provided the amount

complies with the limits or thresholds. For example, PSPs could apply a £40 limit where a €50 limit would apply, for so long as £40 remains less than €50.

20.49 The EBA Opinion (paragraph 42) states that, for example, the limit of five transactions (SCA-RTS 11(c) or SCA-RTS Article 16(c)) needs to be calculated not on the basis of all transactions where the exemption could have been applied but on the basis of transactions where the particular exemption was applied. This reflects the fact that certain transactions may qualify for more than one exemption.

Unattended terminals for transport fares and parking fees (SCA-RTS Article 12)

20.50 PSPs are allowed not to apply strong customer authentication where a payer initiates an electronic payment transaction to pay a transport fare or parking fee at an unattended payment terminal, subject to compliance with the general authentication requirements set out in SCA-RTS Article 2. Where unattended terminals enable contactless payments but the PSP chooses to apply the transport exemption (SCA-RTS Article 12), such activity does not count towards the value and volume limits set by the contactless exemption (SCA-RTS Article 11) since all exemptions are separate and independent.

Trusted beneficiaries (SCA-RTS Article 13)

20.51 Subject to compliance with the general authentication requirements (SCA-RTS Article 2), the PSP can choose not to apply strong customer authentication where a payer initiates a payment transaction (credit transfer or card payment through the payer's PSP, upon the payer's confirmation) to a payee included in a list of trusted beneficiaries set up by the payer. Subject to technical feasibility, application of the exemption is not limited to remote transactions.

20.52 The exemption can be applied where the list of trusted beneficiaries was created prior to 14 September 2019. Strong customer authentication is required when a payer requests its PSP to create or amend a list of trusted beneficiaries. The creation or amendment of such a list may only be done through the ASPSP and not through the services of a PISP or an AISP.

Recurring transactions (SCA-RTS Article 14)

20.53 When a payer creates, amends or initiates for the first time a series of recurring transactions with the same amount and with the same payee (eg a standing order) strong customer authentication is required. Subject to compliance with the transaction monitoring requirements (SCA-RTS Article 2), PSPs are not required to apply strong customer authentication for the initiation of all subsequent payment transactions in the series. A series of recurring payment transactions created prior to 14 September 2019 will only require application of strong customer authentication if the payer subsequently amends it.

20.54 Where a payer sets up a card-based continuous payment authority, strong customer authentication will only be required if the payer initiates the first payment with its PSP, directly or through the payee (for example, where the first in the series of payments is taken immediately). Subsequent payments in the series, which may be for a fixed or variable amount depending upon the agreement between the payer and the payee, are out of scope of the application of strong customer authentication because they are initiated by the payee (eg the merchant) without the involvement of the payer. SCA will not be required, in any event, if the payments taken under the continuous payment authority are all merchant-initiated. Examples of payments where continuous payment authorities may be used include subscriptions (eg for gym membership or digital services), conditional fees (such as hotel cancellation and vehicle rental extended hire fees), utility bill payments and monthly or annual insurance premiums. We encourage merchants to ensure that the continuous payment authority agreement sets out clearly the amount that will be taken in each transaction. We also encourage merchants to give the range within which the amount may vary, if that is a possibility. Regulation 79 of the PSRs 2017 provides certain protections for the payer (see section 8.230 of **Chapter 8 – Conduct of business requirements**). Such remote card payments remain subject to monitoring for the purposes of fraud reporting under the PSRs 2017.

20.55 Direct debits are out of scope of the SCA-RTS, as they are purely payee-initiated. The exception is where the payer's consent is given in the form of an electronic mandate with the involvement of the payer's PSP[90] (for example, this is an option within the Core SEPA Direct Debit Scheme[91]). Strong customer authentication would only be needed for the first in a series of transactions set up in this way.

Credit transfers between accounts held by the same natural or legal person (SCA-RTS Article 15)

20.56 PSPs can choose not to apply strong customer authentication to credit transfers between accounts held by the same payment service user with the same ASPSP, whether that user is a consumer or a business.

Secure corporate payment process and protocols (SCA-RTS Article 17)

20.57 Under SCA-RTS Article 17, PSPs are allowed not to apply strong customer authentication for payments made by payers who are not consumers. This is only the case where the payments are initiated electronically through dedicated payment processes or protocols that are not available to consumers. Furthermore, the FCA must be satisfied that those processes or protocols guarantee at least equivalent levels of security to those provided for by the PSRs 2017. We have set out below how we expect the exemption to be applied and how we intend to monitor its use. This intends to clarify what should meet the level of satisfaction sought by Article 17.

20.58 The exemption may only be applied where the payer using the dedicated payment processes or protocols is a legal person. In our view, this means the payer must be an

90 As noted in paragraph 13 of the EBA final report on the draft RTS

91 https://www.europeanpaymentscouncil.eu/what-we-do/sepa-direct-debit/sdd-mandate

incorporated entity, which would include companies and limited liability partnerships and other entities with legal personality such as NHS Trusts and corporate cooperatives.

20.59 It is also our view that, for example, the use of proprietary automated host-to-host (machine-to-machine) restricted networks[92], lodged[93] or virtual[94] corporate cards, such as those used within an access-controlled corporate travel management or corporate purchasing system, would potentially be within scope of this exemption.

20.60 In our view, the use of physical corporate cards issued to employees for business expenditure in circumstances where a secure dedicated payment process and protocol is not used (eg where online purchases are made via a public website) would not fall within the scope of this exemption.

20.61 Regulation 98 of the PSRs 2017 requires a PSP to provide us with regular, updated and comprehensive assessments of the operational and security risks relating to the payment services it provides and on the adequacy of the mitigation measures and control mechanisms implemented in response to those risks (see **Chapter 18 – Operational and security risks**). PSPs not applying strong customer authentication under SCA-RTS Article 17 must ensure the processes and protocols not subject to strong customer authentication are specifically included in this assessment. This should incorporate a brief description of the payment service, an assessment of the levels of security achieved and a statement by the PSP that those levels of security are equivalent to those provided for by PSD2. Firms intending to operate under this exemption must provide us with this information by including it in an assessment submitted at least 3 months before relying on the exemption. See **Chapter 13 – Reporting and notifications** for more detail.

20.62 To guarantee at least equivalent levels of security to those provided for by PSD2, the dedicated payment processes or protocols must be subject to the application of transaction monitoring (in line SCA-RTS Article 21), fraud prevention, security and encryption measures[95]. These should enable the secure transmission of data and ensure the confidentiality and integrity of the payment service user's personalised security credentials, the identification, verification and authentication of the user, and non-repudiation of the transaction. PSPs should ensure that this is addressed in the above-mentioned assessment sent to us. We expect PSPs to demonstrate that where payments are initiated through use of dedicated payment processes and protocols, their fraud rate, as monitored at least on a quarterly basis in line with SCA-RTS Article 21 and calculated in accordance with SCA-RTS Article 19, is equivalent to, or lower than, the reference fraud rate for the same type of payment transaction indicated in the Annex to the SCA-RTS.

20.63 Where a PSP chooses to apply this exemption, one option would be to obtain an annual independent audit of the dedicated payment processes or protocols which

92 Such networks often employ Public Key Infrastructure-based ('PKI') security systems and may involve a dynamic connection between a company and its banking partners to enable the automated transfer of data to execute payments.

93 Lodged cards are corporate cards 'lodged' securely with a company-approved supplier (eg an office supplies firm) or third-party (eg a corporate travel management company responsible for booking business travel on the company's behalf with merchants such as hotels and airlines) for ongoing business purchases and expenses.

94 Virtual corporate cards are, typically, 16-digit single use or limited multi-use virtual account numbers, with an expiry date and security code, which can only be generated by designated and authorised users acting on behalf of the company for pre-defined transactions.

95 For example, using public key infrastructure, the latest Transport Layer Security and hardware security modules, applying digital signing and signature verification techniques, single use virtual account numbers (VANs) and restricted VAN parameters.

demonstrates PSD2-equivalent levels of security, and an annual certified record of the associated fraud rates . To mitigate against the risk of disruption of services to customers, we encourage PSPs to speak to us at the earliest opportunity if they anticipate any challenges to their compliance so that we can discuss an appropriate way forward with them (see **Chapter 12 – Supervision**).

Transaction risk analysis and calculation of fraud rates (SCA-RTS Articles 18 and 19)

20.64 Subject to the conditions set out in SCA-RTS Article 18, the PSP may choose not to apply strong customer authentication to remote electronic payments identified as posing a low fraud risk having used transaction risk analysis as referred to in SCA-RTS Article 2 and real-time risk analysis referred to in Article 18(2)(c). In line with SCA-RTS Article 18(3), as a minimum PSPs will need to take into account data about the customer's spending patterns and transaction history and be able to identify any abnormal payment patterns. Where the PSP has provided the access device or software, data concerning the location of the payer and payee must also be considered.

20.65 One of the conditions for application of the exemption is that the fraud rate for that type of transaction, calculated in accordance with SCA-RTS Article 19 and monitored in accordance with SCA-RTS Article 21 (see section 20.72 below on monitoring), must be equivalent to or below the appropriate reference fraud rate specified in the SCA-RTS Annex. In addition, the amount of the transaction must not exceed the relevant exemption threshold value ('ETV') specified in the table in the SCA-RTS Annex. For example, if a PSP has a fraud rate of 0.10% for remote electronic card-based payments, that PSP would only be able to apply the exemption to remote electronic card-based payments where the amount was (equivalent to) €100 or less. If its fraud rate was 0.05% for that type of transaction, it could apply the exemption to transaction amounts up to €250. SCA-RTS Article 19(1) requires PSPs to re-calculate their fraud rate once every 90 days, in relation to payment transactions executed during that period.

20.66 The EBA Opinion clarifies that the calculation of the fraud rate should use the same two categories of fraud data that are defined in the EBA Guidelines on fraud reporting.[96] This includes:

- unauthorised payment transactions made, including as a result of the loss, theft or misappropriation of sensitive payment data or a payment instrument, whether detectable or not to the payer prior to a payment and whether or not caused by gross negligence of the payer or executed in the absence of consent by the payer ('unauthorised payment transactions')

- payment transactions made as a result of the payer being manipulated by the fraudster to issue a payment order, or to give the instruction to do so to the PSP, in good-faith, to a payment account it believes belongs to a legitimate payee ('manipulation of the payer').

96 https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-fraud-reporting-under-psd2

Transactions where the payer acted fraudulently are not included in the calculation of fraud rates, in line with the approach taken in the EBA Guidelines on fraud reporting.[97]

20.67 While the fraud rate should be calculated at a PSP (legal entity) level, a PSP may choose to apply the SCA-RTS Article 18 exemption only to specific low risk brands, products and schemes. In scenarios where processing involves more than one PSP, such as card payments, a given PSP's fraud rate should be calculated on the basis of both unauthorised transactions and transactions involving manipulation of the payer which have not been prevented by that PSP. However, the fraud rate calculation does not need to take into account fraudulent transactions for which another PSP has borne sole liability (in accordance with regulation 77(3)(c) and regulation 77(6) of the PSRs 2017).[98]

20.68 While a PSP, such as a card acquirer, may contractually agree to 'outsource' its transaction risk monitoring, e.g. to payees (merchants),[99] wallet providers or gateway providers, only the payee's PSP (acquirer) or the payer's PSP (card issuer) may decide whether to apply the exemption, based on their own fraud rate (see also 20.42).

20.69 The EBA Opinion also clarifies that the fraud rate, which determines whether or not a PSP is entitled to use the transaction risk analysis exemption, is calculated on the basis of that PSP's total remote electronic credit transfers or card-based payments rather than the type of payee or the payment channel used. The calculation and application of the exemption cannot be limited to the total remote electronic credit transfers or card-based payments relating to an individual payee (eg. a specific merchant, even if the card acquirer has contractually agreed to 'outsource' its transaction risk analysis monitoring to that merchant) or for a specific channel (such as an application or web interface). In other words, even if a specific online merchant has a low fraud rate, if the PSP's fraud rate for that transaction type exceeds the reference fraud rate, the PSP cannot apply the SCA-RTS Article 18 exemption to transactions involving that merchant.

20.70 As specified in SCA-RTS Articles 3(2) and 19, the methodology and any model used for the calculation of fraud rates and resulting figures must be documented and audited. Firms should be prepared to provide us with this information upon our request.

Cessation of exemptions based on transaction risk analysis (SCA-RTS Article 20)

20.71 PSPs that use the transaction risk analysis exemption are required to report to us immediately where one of their monitored fraud rates for remote electronic card-based payments or remote electronic credit transfers exceeds the applicable reference fraud rate as set out in the SCA-RTS Annex. SCA-RTS Article 20(2) sets out the conditions around cessation and recommencement of use of the exemption. For example, if a PSP has been applying the transaction risk analysis exemption to remote electronic card-based payments between €250 and €500 and the PSP's fraud rate moves above 0.01%, it will be required to notify us. If the monitored fraud rate exceeds 0.01% for two consecutive quarters, the PSP must cease to apply the exemption to

97 EBA Guidelines on fraud reporting, page 7, paragraph 17
98 EBA Opinion paragraph 46
99 EBA Opinion paragraph 47

remote electronic card-based payments in that value range (ie above €250) until their calculated fraud rate equals or falls below the reference fraud rate applicable for one quarter. Until that happens, provided their fraud rate remains below 0.06%, the PSP may continue to apply the exemption only to remote electronic card-based payments up to €250. Details of the notification requirements can be found in SUP 15.14.29 to 15.14.37. The notification requirement is also summarised in **Chapter 13 – Reporting and notifications**.

Monitoring (SCA-RTS Article 21)

20.72 PSPs that choose to make use of the exemptions set out in SCA-RTS Articles 10 to 18 must record and monitor, on at least a quarterly basis, the following data for each type of payment transaction and according to whether it is remote or non-remote:

- The total value of unauthorised or fraudulent payment transactions in accordance with regulation 67(2)(b) and (c) of the PSRs 2017.
- The total value of all payment transactions and the resulting fraud rate, including a breakdown of payment transactions initiated through strong customer authentication and under each of the exemptions.
- The average transaction value, including a breakdown of payment transactions initiated through strong customer authentication and under each of the exemptions.
- The number of payment transactions where each of the exemptions was applied and their percentage in respect of the total number of payment transactions.

20.73 As specified in SCA-RTS Article 21(2), PSPs should be prepared to provide us with the results of the monitoring, upon our request.

20.74 We expect the transaction totals recorded for the purpose of monitoring to be consistent with the transaction totals recorded and reported for the purpose of meeting fraud reporting requirements under regulation 109 of the PSRs 2017. However, where there are two PSPs involved (e.g. card payments) the monitored unauthorised transactions do not include those for which the other PSP has borne sole liability. Data monitored must include the data on unauthorised transactions and fraudulent transactions resulting from the manipulation of the payer[100] as defined in the EBA Guidelines on fraud reporting. We provide details of how to complete the fraud reporting requirement in SUP 16.13 and **Chapter 13 – Reporting and notifications**.

100 'Manipulation of the payer' refers to payment transactions made as a result of the payer being manipulated by the fraudster to issue a payment order, or to give the instruction to do so to the payment service provider, in good faith, to a payment account it believes belongs to a legitimate payee – https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-fraud-reporting-under-psd2

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 our 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 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 Financial Ombudsman Service.

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 how 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
DisputeResolution:Complaintssourcebook (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.

General Data Protection Regulations 2017 (GDPR)
Information from the ICO about compliance with the GDPR.

Annex 2
Useful contact details

Financial Conduct Authority (FCA)
~~25 The North Colonnade~~
~~Canary Wharf~~
12 Endeavour Square
London, ~~E14 5HS~~
E20 1JN

Contact Centre
0300 500 0597

Consumer Helpline
0800 111 6768

Payment Systems Regulator (PSR)
~~25 The North Colonnade~~
~~Canary Wharf~~
12 Endeavour Square
London, ~~E14 5HS~~
E20 1JN

Contact Centre
0300 456 3677

Consumer Helpline
0800 111 6768

Financial Ombudsman Service
Exchange Tower
Harbour Exchange Square
London, E14 9SR

0800 023 4567 or 0300 123 9123

Her Majesty's Revenue and Customs (HMRC)
National Advice Service
Written Enquiries Section
Alexander House
Victoria Avenue
Southend
Essex, SS99 1BD

0845 010 9000

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

0303 123 1113

Annex 3
Status disclosure sample statements

The following are suggested statements for payment service providers (PSPs) 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 of the Payment Services Regulations 2017 (PSRs 2017) 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) of the PSRs 2017 that the PSP 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 the Financial Services and Markets Act 2000 and the PSRs 2017 should reference both authorisations.

Authorised PIs
[Name] is authorised by the Financial Conduct Authority under the Payment Service Regulations 2017 [register reference] for the provision of payment services.

Authorised EMIs
[Name] is authorised by the Financial Conduct Authority under the Electronic Money Regulations 2011 [register reference] for the issuing of electronic money.

Small PIs/RAISPs
[Name] is registered with the Financial Conduct Authority under the Payment Services Regulations 2017 [register reference] for the provision of payment services.

Small EMIs
[Name] is registered with the Financial Conduct Authority under the Electronic Money Regulations 2011 [register reference] for the issuing of electronic money.

EEA Authorised PIs /-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.

EEA Authorised EMIs
Authorised by [name of Home State regulator] and regulated by the Financial Conduct Authority for the conduct of issuing of electronic money 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 regulation 86(5) of the PSRs 2017, this must be "within the time limits agreed between the payee and its 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 2017 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 PSRs 2017 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(5)). 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.

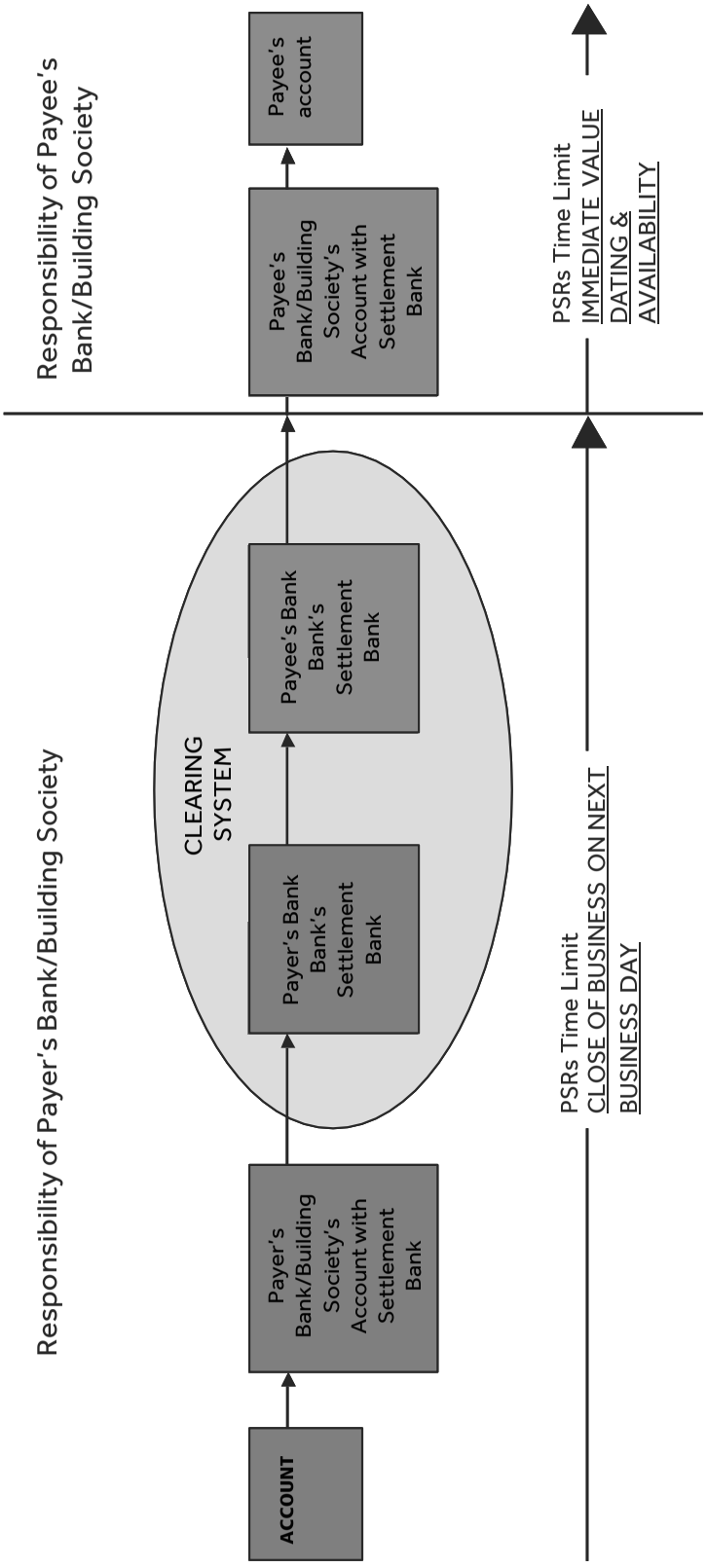
Merchant Acquiring in Three-Party Schemes

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 2017, 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.

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 2017. This is the definition used in the PSRs 2017, 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 references to any of the following persons when they issue electronic money:

- Authorised EMIs
- Small EMIs;
- EEA authorised EMIs;
- Credit institutions;
- The Post Office Limited;

- The Bank of England, the European Central Bank 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.

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 (e.g. where the FCA decides to reject authorisation applications) and supervisory notices (e.g. 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 2017, 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
AIS	Account information service
AISP	Account information service provider
ASPSP	Account servicing payment service provider
ATM	Automated Teller Machine
Authorised EMI	Authorised electronic money institution
Authorised PI	Authorised payment institution
Bacs	Bacs Payment Schemes Limited
BCOBS	Banking Conduct of Business Sourcebook
CAE	Commercial Agent Exclusion
Call for Input	February 2016 Call for Input: the FCA's approach to the current payment services regime
CBPII	Card-based payment instrument issuer
CHAPS	Clearing House Automated Payment System
CONC	Consumer Credit Sourcebook
CP	Consultation paper
CRR	Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms
CSC	Common and secure communications
DEPP	Decision Procedure and Penalties manual
DISP	Dispute Resolution: Complaints
EBA	European Banking Authority
ECB	European Central Bank

~~ECE~~	~~Electronic Communications Exclusion~~
2EMD	Second Electronic Money Directive
AIS	Account information service
AISP	Account information service provider
ASPSP	Account servicing payment service provider
ATM	Automated Teller Machine
Authorised EMI	Authorised electronic money institution
Authorised PI	Authorised payment institution
Bacs	Bacs Payment Schemes Limited
BCOBS	Banking Conduct of Business Sourcebook
CAE	Commercial Agent Exclusion
Call for Input	February 2016 Call for Input: the FCA's approach to the current payment services regime
CBPII	Card-based payment instrument issuer
CHAPS	Clearing House Automated Payment System
CONC	Consumer Credit Sourcebook
CP	Consultation paper
CRR	Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms
CSC	Common and secure communications
DEPP	Decision Procedure and Penalties manual
DISP	Dispute Resolution: Complaints
EBA	European Banking Authority
ECB	European Central Bank
ECE	Electronic Communications Exclusion

EEA	European Economic Area
EG	Enforcement Guide
EMI	Authorised e-money institutions and small e-money institutions
EMRs	Electronic Money Regulations 2011
EU	European Union
FC	Financial Crime: a guide for firms
FCA	Financial Conduct Authority
FEES	Fees manual
FPS	Faster Payments Service
FSA	Financial Services Authority
FSMA	The Financial Services and Markets Act 2000
GEN	The General Provisions of the FCA's Handbook
Handbook	The FCA Handbook of Rules and Guidance, available at http://fshandbook. http://fshandbook.info/
HMRC	Her Majesty's Revenue and Customs
IAP	Indirect Access Provider
ITS	Implementing Technical Standards
LEI	Legal Entity Identifier
LNE	Limited Network Exclusion
MLRs 2007	Money Laundering Regulations 2007
MLRs 2017 (Information	Money Laundering, Terrorist Financing and Transfer of Funds- on the Payer) Regulations 2017
MSB	Money service business
PERG	Perimeter Guidance Manual
PI	Authorised PIs and small PIs
PII	Professional indemnity Insurance

PIS	Payment initiation services

PISP	Payment initiation services provider
POCA	Proceeds of Crime Act 2002
POND	Proportionate objective and non-discriminatory
PRIN	The FCA's Principles for Business
PSD	Payment Services Directive
PSD2	The revised Payment Services Directive
PSP	Payment services provider
PSR	Payment Systems Regulator
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
The ombudsman service	The Financial Ombudsman Service
Treasury	HM Treasury
UNFCOG	Unfair contract terms and consumer notices regulatory guide

Pub ref: 005848
~~Pub ref: 005745~~

~~25 The North Colonnade Canary Wharf London E14 5HS~~12 Endeavour Square London E20 UN Telephone:

+44 (0) 20 7066 1000
Website: www.fca.org.uk