FINANCIAL CONDUCT AUTHORITY

Approach to final Regulatory Technical Standards and EBA guidelines under the revised Payment Services Directive (PSD2)

Consultation Paper
CP18/25**

September 2018

How to respond

We are asking for comments on this Consultation Paper (CP) by Friday 12 October 2018. The consultation period is 4 weeks.

You can send them to us using the form on our website at: fca.org.uk/cp18-25-response-form.

Or in writing to:

Jack Wilson
Financial Conduct Authority
12 Endeavour Square
London E20 1JN

Email:
cp18-25@fca.org.uk

How to navigate this document onscreen

returns you to the contents list

takes you to helpful abbreviations

Contents

1 Summary

Why we are consulting

1.1 The revised Payment Services Directive (PSD2) was implemented in the UK from 13 January 2018. The Directive provides for a number of EU Regulatory Technical Standards (RTS) to be developed by the European Banking Authority (EBA). This consultation paper (CP) focuses in particular on the Regulatory Technical Standards for strong customer authentication and common and secure open standards of communication (SCA-RTS).

1.2 Most of the SCA-RTS provisions have to be applied by firms from 14 September 2019. The SCA-RTS seeks to increase the security of customers' payments made by card and other means. This comes at a time when industry figures put losses due to financial fraud at nearly £1 billion in 2017.

1.3 The SCA-RTS also sets out various requirements that affect what is often termed 'open banking' services. Under PSD2, firms providing account information services (AIS) or payment initiation services (PIS) came within regulation. Provisions in the RTS set out the way AIS and PIS providers can securely connect with customers' banks or other providers to provide their services. They also set out how the FCA and other EU regulators should go about exempting providers, that only build dedicated access interfaces for AIS and PIS providers, from some of the obligations.

1.4 The EBA has also consulted on draft Guidelines on the conditions to be met to benefit from an exemption from contingency measures under Article 33(6) of Regulation (EBA exemption guidelines). These are addressed to both payment service providers (PSPs) and national competent authorities (including the FCA), which have a duty to make every effort to comply with them.

1.5 We are consulting on our domestic implementation before the EBA exemption guidelines are finalised. This is to give stakeholders clarity as soon as possible about what is needed to build systems and seek an exemption in time for 14 September 2019. Our final rules, directions and guidance will take account of any changes made to the EBA exemption guidelines that affect our proposals. We do not intend to consult on any consequential changes unless they are of such significance that it is considered necessary. We have encouraged industry participants to engage in the EBA's consultation on its EBA exemption guidelines. This approach tries to give firms as much notice and certainty as we can about the exemption process and maximises the time available for preparation.

1.6 We are also consulting on new fraud reporting requirements that will affect the data collected and reported by all PSPs. These new requirements implement the EBA Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2) (EBA fraud reporting guidelines).

1.7 Finally, we are taking the opportunity to update our Payment Services and E-Money Approach Document guidance to reflect other legislative changes and clarify our existing expectations based on our experience of the regime (eg, of processing applications) since September 2017. Our proposed amendments and additions are in Annex 3.

1.8 Depending on legislative changes relating to the UK's withdrawal from the European Union, we may need to update our Handbook and guidance relevant to PSD2. Details of the FCA's approach can be found here. The FCA has confirmed its intention to consult on these changes in the Autumn.

Who this applies to

1.9 The proposals apply to PSPs, including banks, building societies, e-money issuers, payment institutions, registered account information service providers and payment initiation service providers.

1.10 The paper will also be of interest to:

- retailers
- consumers and micro-enterprises
- consumer groups
- industry representative bodies
- those involved in open banking initiatives
- Credit Unions – our proposed rules on reporting of data relating to complaints about authorised push payment (APP) fraud would apply to Credit Unions

1.11 This consultation paper (CP) will especially be of interest to firms that are required to provide AIS and PIS providers with access to customers' payment accounts. Those planning to use secure application programming interfaces (APIs) to provide access will be under an additional requirement to provide a 'contingency mechanism' in case of failure of the API. The FCA is required to exempt these firms from this requirement, where we decide certain conditions are met.

1.12 Subject to the outcome of this consultation, the FCA's exemption process will be available in January 2019. Those seeking to be exempt by 14 September 2019 should aim to submit an exemption request by 14 June 2019 (see timeline in Annex 5). This is because we will need time to review the exemption request, and ASPSPs will need further time to allow for building a contingency mechanism prior to 14 September 2019, should we not grant an exemption.

The wider context of this consultation

1.13 This CP forms part of our implementation of PSD2. As the SCA-RTS are directly applicable in the UK, our implementation involves the rules and directions necessary to operationalise the SCA-RTS, and guidance on it in our Approach Document. Details of our previous consultations and policy statements can be found here (PS17/19) and here (CP18/06).

1.14 This consultation looks specifically at the requirement on firms which operate payment accounts online to provide an access interface for third party providers of account information and payment initiation services (TPPs) by September 2019. The firms providing access are called account servicing payment service providers (ASPSPs). This CP also covers the role we have to assess ASPSPs' interfaces to exempt them from some of the requirements of PSD2, where this is appropriate.

1.15 We are implementing PSD2 at the same time as 9 retail banks have been required by the UK Competition and Markets Authority to develop application programming interface (API) standards (referred to as 'open banking'). The standards facilitate the access to customers' current account data by TPPs required under PSD2. This work is being coordinated by the Open Banking Implementation Entity (OBIE). The OBIE recently published standard implementation requirements for firms using its API standards. These standards are aimed at ensuring that firms' APIs are aligned with the requirements and objectives of PSD2.

1.16 We also consider our approach to rules, effective from 14 September 2019, requiring all PSPs to ask customers for more information in order to verify their identify before a payment is made. This 'strong customer authentication' will be a requirement unless an exemption is used (eg, for low value payments).

What we want to change

1.17 This CP proposes new rules, and a number of changes and additions to the guidance on PSD2 in the Payment Services and E-money Approach Document (Approach Document) and Perimeter Guidance Manual (PERG) to ensure:

- We can exempt ASPSPs from the requirement to build a contingency mechanism ahead of 14 September 2019, after which it will become a requirement unless an exemption has been obtained.
- We can receive the information that PSPs are required to provide under the finalised SCA-RTS in a consistent format.
- Our Approach Document guidance on PSD2 is up-to-date with the SCA-RTS and the Passporting RTS published on 11 November 2017.
- Our Approach Document guidance is aligned with EBA exemption guidelines (once they are final) and the EBA's published Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC.
- Our Approach Document guidance on the authorisation process reflects our practical experience of authorising and registering firms under PSD2.

- Complaints reporting rules are extended to cover authorised push payment fraud.

- Issues which have been identified by stakeholders or by the FCA since the previous PSD2 Policy Statement was published are addressed, including some changes to the Perimeter Guidance Manual (PERG).

1.18 We also consult on fraud reporting rules following the publication of EBA fraud reporting guidelines.

1.19 We do not detail every minor change to the Approach Document in the text of this CP. Please read this CP with the revised Approach Document in Annex 3 (with marked-up changes) and rules and Perimeter Guidance in Appendix 1.

Outcome we are seeking

1.20 We want ASPSPs to implement PSD2 using well-functioning, secure APIs. A standardised set of APIs have already been developed by the OBIE. We believe the use of standardised APIs will have benefits for market participants and consumers and we encourage their adoption. Once APIs are in use in the market and working well, we expect it should no longer be necessary for firms to rely on practices that mean customers share their banking credentials with third parties (referred to as 'screen scraping').

1.21 The additional guidance we are proposing should also lead to more consistent implementation of the requirements of PSD2 by PSPs, helping to ensure that the key objectives of PSD2 are met. These are aligned with the FCA's objectives and include achieving enhanced consumer protection, promoting innovation and improving the security of payment services. Our implementation aims to support the success of new AIS and PIS services, leveraging the work of the OBIE to deliver this.

Measuring success

1.22 We have already introduced reporting that will help us to track the take-up of the services provided by newly-regulated PIS and AIS providers. These further proposals should encourage wider use of these services, which we will be able to track. We will also consider the number of successful exemption requests as an indicator of success.

Next steps

What you need to do next

1.23 We want to know what you think about our proposals. Please send us your comments by Friday 12 October 2018. You can use the online response form on our website or write to us at the address on page 2.

What we'll do next

1.24 We will consider your feedback and then publish any finalised rules and guidance.

2 The wider context

Open banking and APIs

2.1 One aim of PSD2 is to enhance competition in payment services by supporting providers of account information services (AIS) and payment initiation services (PIS) by bringing these services within the scope of regulation. These firms are collectively known as third-party providers (TPPs). Once regulated, they will have the right to access customers' payment account data and payment functionality, if they have the customer's explicit consent.

2.2 With this access TPPs can provide services to customers which previously only banks might have provided. At present, most of these TPPs access customers' accounts directly by asking the customer to input their banking credentials. The TPPs log onto customers' accounts as if they are the customer. This allows them to 'scrape' data from the account to provide services to the customer, or to make payments on their behalf.

2.3 From 14 September 2019, all account servicing payment service providers (ASPSPs) – such as banks and other PSPs providing and maintaining an online payment account for a customer – will have a choice as to whether TPPs can access customer accounts directly (using their credentials), or via dedicated interfaces. The latter will enable the customer to be redirected[1] to their bank or PSP to provide credentials. This ensures that customer credentials never have to be provided to anyone other than a customer's bank or PSP.

2.4 In a joint statement with the Treasury in July 2017 we made clear that we support the implementation of PSD2 using application programming interface-based dedicated interfaces (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.

2.5 This consultation looks specifically at the requirement on ASPSPs to provide an access interface (including using APIs) by 14 September 2019. It also covers the role we have to assess whether ASPSPs' interfaces satisfy the relevant conditions in the Regulatory Technical Standards on strong customer authentication and common and secure open standards of communication (SCA-RTS) in order to exempt them from some of the requirements of PSD2.

2.6 We want to encourage ASPSPs to comply with PSD2 by implementing standardised APIs. Such APIs have already been developed by the Open Banking Implementation Entity (OBIE). We believe the use of standardised APIs will have benefits for market participants and consumers. The requirement to build a contingency mechanism (ie a second means of access for TPPs) in addition to an API interface will pose extra costs

1 Other alternative access approaches are being considered, such as 'de-coupled' – see draft Approach Document in Annex 3, section 17.118.

for ASPSPs. The SCA-RTS allows ASPSPs to be exempted from this requirement (and the related costs). This aims to provide ASPSPs with an incentive to build good APIs. We therefore encourage ASPSPs to seek exemption. We are consulting on our proposed approach to the exemption process in this document.

Security of electronic payments

2.7 PSD2 also aims to prevent harm to consumers caused by payments fraud. It introduces measures to strengthen the process of authorising a payment. It requires all PSPs to report payment fraud statistics so that regulators can address fraud trends or problem areas. These requirements should enhance consumer protection and market integrity, in line with our FCA objectives.

2.8 From 14 September 2019, all PSPs will need to ask customers for more information in order to verify their identify before a payment is made. This 'strong customer authentication' will be a requirement unless an exemption is used (eg, for low value payments).

2.9 These measures are designed specifically to combat unauthorised payments, which can be made eg, when credit or debit cards are lost, stolen or otherwise compromised. This issue is important to us, with estimated losses to card fraud in the UK of £566 m in 2017.

2.10 At the same time, the UK industry has started to track fraud resulting from authorised push payment (APP) scams. This is where customers unknowingly authorise payments to fraudsters eg, where the payer intends to transfer the funds to a particular person but is instead deceived into transferring funds to a different person.

2.11 Data on APP fraud show there were 43,875 cases in 2017, with total losses of £236 m. Of these cases, 88% involved consumers who lost on average £2,784 per case, and the remaining 12% were businesses that lost on average £24,355 per case.

2.12 To align with work the FCA and Payment Systems Regulator have been doing on APP scams, we are consulting on collecting data about customers' complaints about APP fraud. We also propose to refer in our Approach Document to industry work on a contingent liability code on such fraud.

Consumer protection

2.13 Our proposals to implement PSD2 should help to protect consumers eg, by further strengthening the security of payments, and increasing transparency around the scale of payments fraud.

Market integrity

2.14 The changes we propose should enhance market integrity by introducing measures to address threats to the security of electronic payments. This should help to improve trust in the financial system. We also include proposals on further guidance for firms seeking authorisation. This is to make sure new firms entering the market have a full understanding of their regulatory obligations.

Competition

2.15 PSD2 looks to drive competition in retail banking and payments. The first Payment Services Directive introduced a new class of payment institutions to compete with banks for the provision of payment services. PSD2 introduces another new class of

regulated entity (account information services provider or payment initiation service provider) to compete in the space between a bank and its customer, to provide value added services and unlock the potential of payment account data and functionality. The proposals in this consultation are about how these TPPs can access customers' payment accounts held with their bank in a secure, frictionless and effective manner. Our market studies into the credit card market and cash savings have both referenced the potential benefit that such services could bring by improving choice and competition.

Wider effects of this consultation

2.16 We are implementing legal requirements stemming from EU rules. The requirements in the SCA-RTS could lead to changes or additional steps to the way customers pay for things online.

2.17 If the competition objectives of PSD2 are met through our implementation, including proposals in this CP, in the long term the relationships customers have with their banking providers could change. For example, customers might be less reliant on their banking apps or websites to manage their finances because they may use third party apps which could potentially provide better services.

2.18 The ability of third party apps to interrogate a customer's transaction information could lead to customers being provided with tailored recommendations for products beyond banking, including utilities, subscriptions and other products or services where the charge appears on a bank statement.

What we are doing

2.19 We are seeking your views on our proposals set out in paragraph 1.17, which are explained further in Chapters 3 to 6.

Equality and diversity considerations

2.20 We believe that our proposals will have a positive impact on all consumers, including those with protected characteristics. Depending on the outcome of the work proposed, we would see open banking products being implemented so that customer journeys are relatively seamless, while still being secure and trustworthy. This should encourage take up of the products among a range of demographics.

2.21 We are mindful, however, that take up of new online services is likely to be lower among those without online access or the estimated 9.6 million consumers with low digital capabilities.

2.22 Equally, we have considered that the impact of the new legislation might vary between age groups. For instance, take-up should be greater among those who trust sharing their data. 85% of 18-24 year olds would trust third parties to aggregate their financial data whereas 48% of 55-64 year olds were neutral or positive.

3 Secure communication between payment account providers and third-party providers (TPPs)

3.1 This chapter focuses on our proposed approach to elements of the final Regulatory Technical Standards for strong customer authentication and common and secure open standards of communication (SCA-RTS) which relate to the secure communication between account servicing payment service providers (ASPSPs), account information and payment initiation service providers, and card-based payment instrument issuers (collectively referred to as third-party providers (TPPs)).

3.2 The SCA-RTS sets out how TPPs and ASPSPs should interact and communicate securely to enable TPPs to provide their services to customers with their consent.

3.3 After the SCA-RTS was finalised, in June 2018 the EBA published its Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC (EBA Opinion). It also published draft Guidelines on the conditions to be met to benefit from an exemption from contingency measures under Article 33(6) of Regulation (EBA exemption guidelines).

3.4 The EBA exemption guidelines set out how we should approach exempting ASPSPs from having to build an additional access interface that TPPs would use in the event there is a problem with the main 'dedicated interface'. Firms do not have to provide this 'contingency mechanism' if we are satisfied that their dedicated interface meets the criteria for exemption set out in the SCA-RTS.

3.5 This chapter also discusses changes we propose to the Payment Services and E-Money Approach Document to reflect these EBA exemption guidelines and the EBA Opinion. We are consulting based on the draft guidelines in order to give industry as much time as possible to prepare.

Exemption from the contingency mechanism

3.6 By 14 September 2019, any provider offering payment accounts that are accessible online (bank and e-money accounts, credit card accounts, some savings accounts) must comply with the SCA-RTS governing how TPPs can access these accounts.

3.7 These ASPSPs must decide whether to enable access via a dedicated interface built on APIs (application programming interfaces) or whether they adjust the customer interface (ie, the customer online banking portal) to comply with rules around security, information exchange and identification.

3.8 The SCA-RTS allows competent authorities to exempt providers that are building dedicated interfaces from having to provide a 'contingency mechanism' which would provide 'fall-back' access if the dedicated interface failed. Unless ASPSPs have been granted this exemption in advance of 14 September 2019, based on the quality of access provided by the interface outlined below, they will have to build a contingency mechanism.

3.9 The SCA-RTS sets out the conditions that must be met for an ASPSP to be granted an exemption. The EBA exemption guidelines specify the conditions which the FCA should assess as having been met in order to exempt ASPSPs.

Our proposals

3.10 The EBA exemption guidelines describe the criteria ASPSPs need to meet to be granted an exemption. The criteria cover:

- the service level, availability and performance of the dedicated interface, including the publication of indicators
- the adequate stress testing of the dedicated interface
- the design and testing of the dedicated interface, particularly to ensure this does not create obstacles to TPPs
- the wide use of the dedicated interface
- the resolution of problems identified during design, testing and use

3.11 The EBA exemption guidelines do not specify how evidence of compliance should be provided to competent authorities or what exactly the information should be in all cases.

3.12 We propose to require ASPSPs to submit an exemption request form with specific information in order for us to make an assessment (see directions and the draft form in Appendix 1).

3.13 We also propose guidance in Chapter 17 of the Approach Document to help ASPSPs understand the exemption process (see Annex 3). These changes follow from the EBA exemption guidelines. Some of the most substantive changes cover:

- **Timeline for exemption** – subject to the outcome of this consultation, the process will be available from January 2019. Those seeking to be exempt by 14 September 2019 should consider how long they might need to develop a contingency mechanism in the event that an exemption request is rejected. We would expect to receive exemption requests by 14 June 2019 (see timeline in Annex 5). This would allow enough time for us to assess a request. We aim to take no more than 1 calendar month to assess an exemption request. Should a request be unsuccessful, the ASPSP would then have 2 months to develop a contingency mechanism. We encourage firms to contact us well before submitting the exemption request in order to minimise the chances of it being unsuccessful.
- **How we will take account of conformance testing undertaken by ASPSPs as part of the exemption assessment** – we set out how work of market initiatives, including the Open Banking Implementation Entity (OBIE), to facilitate 'conformance testing' of ASPSPs' interfaces will inform our own assessment for the purposes of the exemption.
- **Submission of exemption request** – firms with multiple dedicated interfaces, ie, for each brand within a group, should submit 1 exemption request per dedicated interface.

- **Design and testing** – ASPSPs must have made technical specifications and testing facilities available to TPPs no later than 14 March 2019. The testing facilities must meet requirements (a)-(f) in EBA Guideline 6.2.

- **Wide use** – we will expect ASPSPs, where possible, to have provided operational dedicated interfaces that have been used by TPPs with customers for 3 months before an ASPSP seeks exemption. If it is not practically possible to do so fully in advance of September 2019, ASPSPs should be able to show that they have taken steps to encourage the use of the interface and publicised the availability of the testing facilities for a minimum of 3 months before seeking the exemption.

- **Market initiatives** – we will take account of whether ASPSPs have followed the standard implementation requirements of an industry initiative, such as OBIE. Where this is not the case we will require additional information to enable us to consider more closely whether such implementations are compliant with the PSD2 requirements.

3.14 Under the SCA-RTS, ASPSPs are required to publish quarterly statistics on the availability and performance of their dedicated interfaces and, for comparison purposes, of the interfaces used by their payment service users.

3.15 We also propose to require ASPSPs to submit the quarterly statistics to us quarterly (see Annex 3). This will help us to monitor whether ASPSPs are meeting their obligations to ensure that dedicated interfaces are performing at least as well as the interfaces customers use to access their accounts directly.

Q1: **Do you agree with our approach to assessing requests for exemption to the contingency mechanism and our related guidance? If not, please explain why.**

Q2: **Do you agree with our proposal to require quarterly submission to us of the quarterly statistics ASPSPs are required to publish under the SCA-RTS? If not, please explain why.**

Problems with the dedicated interface

3.16 Under the SCA-RTS, both ASPSPs and TPPs must report problems with dedicated interfaces to the FCA. This information will be used as part of our ongoing assessment of whether an ASPSP is meeting its obligations under the SCA-RTS and, if relevant, whether the ASPSP should continue to be exempt from the requirement to build a contingency mechanism.

Our proposals

3.17 In order to receive and record these reports in a consistent manner, we propose a reporting direction and a specific reporting form (see Appendix 1).

3.18 We also propose changes to Chapter 13 and Chapter 17 of the Approach Document to provide further information and guidance on the reporting process and the information we require (see Annex 3).

Q3: **Do you agree with our approach to receiving reports about problems with dedicated interfaces? If not, please explain why.**

Other changes to guidance on secure communication between payment account providers and third-party providers

3.19 The SCA-RTS sets general and specific requirements for identification, the traceability of transactions, the security of communication sessions and the exchange of data between ASPSPs and TPPs. The EBA Opinion provides additional clarity on certain points to aid implementation of the SCA-RTS.

3.20 To reflect the EBA Opinion and the SCA-RTS in our approach to the secure communication between ASPSPs and TPPs, we propose a number of changes to our Approach Document in addition to those outlined above. These changes cover:

- the type of information the ASPSP should consider when determining the response to a request for confirmation of availability of funds – see Approach Document Section 17.23 in Annex 3
- the scope of information that payment initiation service providers (PISPs) may receive to help them to manage the risk of non-execution of a payment – see Approach Document Section 17.26 to 17.29 in Annex 3
- the scope of the data that account information service providers (AISPs) can access – see Approach Document Section 17.32, 17.64 and 17.72 in Annex 3
- the 4 times per day limit for AIS access where the customer is not actively involved – see Approach Document Section 17.73 in Annex 3
- further clarification about the level of payment functionality available when the customer uses a PISP – see Approach Document Section 17.35 in Annex 3
- the qualified certificates that need to be exchanged between ASPSPs and TPPs for identification – see Approach Document Section 17.56 in Annex 3
- access to customers' personal identifying information – see Approach Document Section 17.33 information in Annex 3

3.21 We have made a number of other changes to Chapter 17 and Chapter 8 and developed a new Chapter 20 so that the Approach Document reflects the final SCA-RTS, the EBA exemption guidelines and the EBA Opinion. In addition, we have included clarification in response to issues raised by payment service providers and other stakeholders. These changes can be viewed as tracked changes in Annex 3.

Q4: **Do you agree with our changes to the Approach Document to reflect the EBA exemption guidelines, EBA Opinion and the SCA-RTS? If not, please explain why.**

4 Authentication

4.1 This chapter focuses on our proposed approach to the final Regulatory Technical Standards for strong customer authentication and common and secure open standards of communication (SCA-RTS) where they relate to requirements for strong customer authentication.

4.2 From 14 September 2019, all payment service providers (PSPs) must comply with regulation 100 of the PSRs 2017 regarding authentication of payments and with the SCA-RTS requirements. These require a PSP to undertake strong customer authentication with a customer (unless one of the permitted exemptions applies) where a customer:

- Accesses their payment account online, whether directly or through an account information service provider (AISP) or payment initiation service provider (PISP);
- 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.

4.3 The Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC (EBA Opinion) published on 13 June 2018 provided further clarity regarding the implementation of the SCA-RTS requirements.

4.4 This chapter discusses the addition of a new Payment Services and E-Money Approach Document chapter covering authentication (Chapter 20). We also discuss proposals to reflect the EBA Opinion where it covers elements of the SCA-RTS relating to use of the permitted exemptions from the application of strong customer authentication.

Notification when the fraud rate is exceeded

4.5 Under the SCA-RTS, PSPs must apply strong customer authentication to remote electronic payments unless a relevant exemption applies. PSPs making use of any of the exemptions are also required to monitor their rates of fraud.

4.6 Where a PSP makes use of the transaction risk analysis exemption it must notify its competent authority when a monitored fraud rate exceeds the applicable reference fraud rate.

Our proposals

4.7 To receive and record these notifications in a consistent manner, we propose reporting rules and a specific notification form (see Appendix 1).

4.8 We also propose additions to the Approach Document to clarify what information we expect to receive and in what circumstances the reports should be provided.

4.9 Our guidance clarifies that, as per the EBA Opinion, we will expect PSPs to calculate the fraud rate using fraud as recorded under the EBA Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2). This means using both 'unauthorised transaction' and 'manipulation fraud' as defined in the EBA fraud reporting guidelines to calculate the fraud rate.

4.10 The proposed report will be used for both notifications that the fraud rate has been exceeded and notifications that the fraud rate has been restored to the applicable level, before a PSP begins to operate under the transactional risk analysis exemption again.

Q5: Do you agree with our approach to receiving notifications relating to the fraud rate? If not, please explain why.

SCA exemption for corporate payments

4.11 Under the SCA-RTS, PSPs are allowed to not 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 PSD2.

Our proposals

4.12 We propose to clarify the scope and conditions of application of this exemption (see Approach Document Sections 20.55 to 20.60 in Annex 3).

4.13 We also propose to direct PSPs applying the exemption to include details of these dedicated processes and protocols not subject to strong customer authentication in the assessment of operational and security risks which is already required under regulation 98 of the PSRs 2017 (see Approach Document Sections 13.5 and 18.16 in Annex 3). This report is already sent to the FCA on an annual (or more frequent) basis.

Q6: Do you agree with our proposed approach to the corporate payment exemption? If not, please explain why.

Other changes to our guidance on strong customer authentication

4.14 The SCA-RTS sets out the criteria that need to be met to satisfy the requirements for strong customer authentication. In the case of electronic remote payments this includes a requirement to dynamically link the transaction to a specific amount and a payee. The SCA-RTS also specifies the conditions where the PSP is allowed not to apply strong customer authentication, ie permitted exemptions.

4.15 To reflect the SCA-RTS and the additional clarification provided by the EBA Opinion, we propose a number of other changes to our Approach Document to cover, among other things:

- **use of two-factor authentication** – we clarify that, in line with the EBA Opinion, strong customer authentication factors need to be from separate categories. We also discuss the use of card verification numbers as a possession factor – see Sections 20.14 to 20.21 of the Approach Document

- **application of strong customer authentication** – we refer to the EBA Opinion's clarification on the application of strong customer authentication when a PSP is outside of the EEA. We also cover a TPP's reliance on credentials issued by an ASPSP in a redirection journey

- **authentication code** – we note that the authentication code does not have to be visible to the payment service user, providing certain requirements are met

- **exemptions from strong customer authentication** – we set out our views on each of the exemptions from strong customer authentication (see Sections 20.36 to 20.65 of the Approach Document in Annex 3). This includes:

  - clarifying the application of the payment account information exemption and the associated 90-day limit in the context of access by an AISP – see Sections 20.41 to 20.45 of the Approach Document in Annex 3

  - clarifying the limit conditions set by the exemptions for 'contactless payments at point of sale' and 'low-value transactions' – see Sections 20.46 to 20.47 of the Approach Document in Annex 3

  - clarifying that the exemption for trusted beneficiaries is not limited to credit transfers – see Sections 20.49 to 20.50 of the Approach Document in Annex 3

  - setting out our expectation that PSPs should use transactions reported under the EBA fraud reporting guidelines as the basis for calculating the fraud rate. This means counting both unauthorised transactions, and transactions as a result of manipulation of the payer, as defined under the EBA fraud reporting guidelines – see Section 20.63 of the Approach Document in Annex 3

  - covering the requirement to monitor data on unauthorised and fraudulent transactions for PSPs making use of the exemptions to strong customer authentication. PSPs are required to provide these data on request to either the FCA or EBA – see Section 20.68 of the Approach Document in Annex 3.

Q7: **Do you agree with our proposed approach to the application of the strong customer authentication requirements and associated exemptions? If not, please explain why.**

5 Fraud and complaints reporting

5.1 Since we published our approach to fraud reporting under PSD2 in September 2017, there have been a number of relevant developments. The European Banking Authority (EBA) has concluded its work to introduce its Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2) (EBA fraud reporting guidelines) that aim to harmonise reporting across the EU. The FCA and the Payment Systems Regulator (PSR) have also continued work to address authorised push payment fraud (APP fraud). This section discusses changes we propose relating to both developments.

Changes to fraud reporting following final EBA fraud reporting guidelines

5.2 PSD2 requires PSPs to provide to their competent authorities, at least annually, statistical data on fraud relating to different means of payment. Competent authorities are required to provide these data in aggregated form to the EBA and European Central Bank (ECB).

5.3 The Directive does not specify what these statistical data should include or how the data should be reported.

5.4 As such, in September 2017, we published final rules to require all PSPs, from 13 January 2018, to collect the fraud data specified in Form REP017, on an annual basis.

5.5 At that time, the EBA was developing fraud reporting guidelines, to harmonise the reporting across the EU, but these were not in place in time for firms to start recording data under them from 13 January 2018. We said at the time that once the EBA finalised its guidelines, we would update our approach (eg, how and when we would replace REP017).

5.6 The EBA fraud reporting guidelines were finalised in July 2018. We support the intention of these guidelines – to collect important data on fraud. We propose to replace REP017 with an updated form that reflects these guidelines.

5.7 Responses to the EBA consultation on the fraud reporting guidelines and subsequent discussions within the FCA's PSD2 Stakeholder Liaison Group suggest that certain of the more detailed elements of the reporting required by the guidelines would impose considerable burdens on some PSPs. Nevertheless, to date we have not received sufficiently compelling evidence from stakeholders to convince us that we should not comply with the guidelines.

Our proposal

5.8 We propose changes to SUP 16 to direct payment service providers (PSPs) to submit a new form replacing REP017. The proposed new REP017 form and draft notes on how to complete it can be found in Appendix 1. The FCA is under a duty to make best efforts to comply with such guidelines. Nonetheless we are keen to understand from stakeholders any practical challenges or concerns that might be faced in implementing the guidelines.

5.9 The EBA fraud reporting guidelines do not require account information service providers (AISPs) to report fraud data. However, the Payment Services Regulations (PSRs) 2017 require all PSPs, including AISPs to report statistical data on fraud resulting from their own services. To help AISPs to comply with this requirement, we will continue to request fraud data from AISPs. Details on the data we propose to collect from AISPs can be found in Appendix 1.

5.10 We will direct banks, building societies, authorised payment institutions and authorised e-money institutions to provide 6 monthly data. This is a change from our current requirements for annual reporting for all PSPs. We believe that the frequency of reporting set out for different firms in the EBA fraud reporting guidelines is proportionate. It will allow the FCA to monitor more up-to-date data more frequently for larger firms reporting. Small payment institutions and small e-money institutions will be directed to report the data annually but this will still have to be broken down into 6 month periods according to the guidelines.

5.11 We propose changes to Chapter 13 – on reporting and notifications in the Payment Services and E-Money Approach Document (Approach Document) – to reflect the new reporting requirements.

5.12 We are also considering how to make use of the data (other than for Supervision) in ways which can be beneficial for PSPs and consumers. We welcome feedback from PSPs on whether sharing anonymised, aggregated data with PSPs and their trade bodies would be beneficial and whether PSPs would find it useful for us to publish the data in an aggregated form.

Q8: **Do you agree with our approach to implementing the EBA fraud reporting guidelines? If not, please explain why.**

Q9: **Do you have any feedback on how the FCA can best use the data we would receive under the EBA fraud reporting guidelines?**

Introduction of complaints reporting relating to APP fraud

5.13 This section is relevant to both PSPs subject to the PSRs 2017 and to credit unions.

5.14 On 23 September 2016, Which? submitted a Super Complaint to the PSR, which was also sent to the FCA regarding the consumer safeguards for authorised push payments. Which? had concerns that there is currently insufficient protection in place for consumers who have been victims of fraud where the customer authorises a payment (in contrast to unauthorised payments ie, where a stolen credit card is used to make payments). Which? noted that consumers making other types of payment have more protections. For example, card payments (under the Consumer Credit Act 1974); 'chargeback rules' for debit cards; and direct debits (under the Direct Debit Guarantee).

5.15 An authorised push payment occurs where the customer gives their consent for a payment to be made, usually by credit transfer, from their account to another account. APP frauds involve the customer being tricked, eg, into consenting to a payment being sent to a fraudster's account, rather than an intended recipient.

5.16 In June 2018 (CP18/16), we consulted on rules to require PSPs and credit unions to handle complaints where they have received funds that have been transferred as a result of an alleged APP fraud in line with the Dispute Resolution: Complaints sourcebook (DISP).

5.17 We also proposed to allow eligible complainants to refer these complaints to the Financial Ombudsman Service if they are unhappy with the outcome reached by the PSP, or if they have not received a response to the complaint.

5.18 CP18/16 included a draft definition of APP fraud, which can be found in Appendix 1. It should be noted that APP fraud is not the same as 'manipulation fraud' which is required to be monitored and reported by PSPs under PSD2.

5.19 In April 2017 (CP17/11), we consulted on rules to require all PSPs to report data on complaints about payment services and e-money, using a new reporting form called 'The Payment Services Complaints Return'. At that point, we proposed that the data reported to us should describe which types of payment service the complaint was about. The proposals did not ask PSPs to provide any information about APP fraud complaints.

Our proposal

5.20 We now propose to require all firms and PSPs to record and report data on complaints they have received about alleged APP fraud using the Payment Services Complaints Return (see Appendix 1). Because credit unions may also be the recipients of funds transferred as a result of APP fraud, we are proposing to amend credit union complaints reporting rules. This is the only proposed rule in this CP relevant to credit unions. These data may be reported externally on the FCA website, and would be visible to PSPs and consumers.

5.21 We propose to add relevant fields to the Payment Services Complaints Return as illustrated in Appendix 1 and the Credit Union Complaints Return, also in Appendix 1.

5.22 We will use these data to understand whether there has been progress on tackling APP fraud, and to inform our supervisory work.

Q10: **Do you agree with our proposal to require PSPs and Credit Unions to record and report data on complaints they have received about alleged APP fraud in general? If not, please explain why.**

Additions to guidance related to APP fraud

5.23 We have also made some changes to Chapter 8 (Conduct of Business) of our Approach Document, relating to APP fraud and related regulatory and industry initiatives. These are discussed below.

Misdirected payments

5.24 Under PSD2, where a payment service user authorises a payment to the wrong sort code and account number, PSPs are required to make reasonable efforts to recover the funds. The payee's PSP must co-operate with the payer's PSP in its efforts to recover the funds, specifically by providing all relevant information to the payer's PSP.

A similar problem with recovery of funds can occur whether a customer themselves is defrauded into sending funds to the wrong sort code and account number or does so mistakenly.

Our proposal

5.25 The same cooperation should be put in place whether the payment service user provides an incorrect sort code and account number by mistake or as a result of being deceived into providing the account number and sort code of an account held by a person other than the person they intend to send the money to. We propose to clarify this in the Approach Document – see Section 8.296 in Annex 3.

Q11: **Do you agree with our proposed Approach Document text clarifying our expectations in relation to PSPs' requirements where the wrong unique identifiers are used? If not, please explain why.**

Clarifying guidance in light of the contingent reimbursement code

5.26 Where customers pay using credit transfers, the payment type requires that the customer will have authorised the payment to 'push' funds to the payee. Under PSD2, it is the customer's responsibility to provide the correct sort code and account number when making a credit transfer. A customer may not be entitled to be reimbursed by its PSP, even where they have inadvertently sent money to the wrong account.

5.27 The Which? Super Complaint has drawn attention to scenarios where a customer has authorised a payment by providing account details to their PSP, but has been subject to a scam.

5.28 The PSR has established a steering group, consisting of PSPs and consumer representatives, that is developing a voluntary contingent reimbursement industry code that would help to address cases of customer harm due to APP fraud. Under this code, if a PSP could have taken steps to prevent instances of APP fraud (such as shutting down the accounts of fraudsters, or implementing confirmation of payee), the PSP will voluntarily help to reimburse those customers.

Our proposal

5.29 We propose to refer to the development of the contingent reimbursement code in our Approach Document (see Section 8.297 in Annex 3). We will also remind PSPs that they are under an obligation to comply with legal requirements to deter and detect financial crime as detailed in Approach Document Chapter 19 – Financial Crime.

Q12: **Do you agree with our proposed Approach Document text clarifying guidance in light of the contingent reimbursement code developments? If not, please explain why.**

6 Other changes to the Approach Document

6.1 We propose several consequential changes to various chapters of the Payment Services and E-Money Approach Document. These will ensure the Approach Document remains up-to-date, following a number of other EU Regulatory Technical Standards and guidelines that have been finalised, and following our experience since we published the Approach Document in September 2017. The changes are as set out below:

Introduction (Chapter 1)

6.2 We propose to update the introduction chapter to reflect that:

- the Regulatory Technical Standards for strong customer authentication and common and secure open standards of communication (SCA-RTS) are now final
- deadlines for firms to be re-authorised or re-registered under PSD2 in order to continue operating have now passed or will have.

Authorisations (Chapter 3)

6.3 We propose changes to guidance on the process for authorisation under PSD2. These changes reflect our experience of authorising and registering firms since October 2017. The proposed changes can be found in tracked changes in Annex 3 and include:

- clarifying the information needed in applications
- providing further examples in the guidance to help those applying to understand the requirements for PSD or EMD individuals
- clarifying what should be covered by professional indemnity insurance

Passporting (Chapter 6)

6.4 When we published the Approach Document in September 2017, we included a chapter on passporting. This was based on draft Regulatory Technical Standards 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). We said we would update the Approach Document after the Passporting RTS are published in the Official Journal and take effect. The Passporting RTS has now been published. We propose to update the Approach Document accordingly.

Conduct of business (Chapter 8)

6.5 We have made some changes to Chapter 8 to align it with rules and guidance which were in draft when we published the Approach Document, but which are now final. Some of these changes reflect developments in the market or industry requests for clarity. We have also made the changes relating to authorised push payment (APP) fraud discussed in the previous chapter.

Reporting and notifications (Chapter 13)

6.6 We have proposed amendments to Chapter 13 to include information on how to submit the additional notifications and new or additional reports discussed above. The Chapter 13 changes should help sign-post firms to the relevant rules, guidance or submission methods.

Q13: **Do you agree with our other changes to the Approach Document? If not, please explain why. Please provide section references in your response.**

7 Other changes to Perimeter Guidance and Handbook

7.1 Following publication of our Policy Statement in September 2017, we have identified the need for some changes and corrections to our Perimeter Guidance Manual (PERG).

Agents of registered account information service providers (RAISPs)

7.2 Under regulation 34 of the Payment Services Regulations (PSRs) 2017 (as amended by The Payment Systems and Services and Electronic Money (Miscellaneous Amendments) Regulations 2017 SI 1173/2017) authorised payment institutions, small payment institutions and registered account information service providers (RAISPs) may not provide payment services through an agent unless the agent is registered with the FCA.

7.3 An agent is a person who acts for a payment institution (PI), e-money institution (EMI) or RAISP (their 'principal') in the provision of payment services.

7.4 The principal is responsible for all their agents' activities when they are providing the principal's service. The PSRs 2017 require payment service users to be informed of the agency arrangement, as well as the name of the payment service provider (PSP). This means that it should always be clear to a customer that they are receiving the principal's service through an agent, and who the principal is. This is important because the customer will have a right of recourse if something goes wrong with the principal. An agent that provides payment services to customers on its own behalf rather than for its principal is likely to be in breach of the prohibition in regulation 138 of the PSRs 2017 (prohibition on provision of payment services by persons other than PSPs) and would need their own authorisation or registration.

Proposal

7.5 For account information services there may be more than one business involved in obtaining, processing and using payment account information as part of providing an online service to a customer. We are proposing additional guidance to clarify how agency arrangements might work in these circumstances and more generally to cover other PSPs.

7.6 An AISP can appoint an agent, but because an agent can only provide its principal's payment services, the agent cannot provide account information services in its own right. This means that if an AISP (Firm A) passes payment account data to another firm (Firm B), and Firm B uses that data to provide account information services (AIS) to its customers, Firm B must be authorised or registered with permission to provide AIS.

7.7 However, if Firm B is acting as Firm A's agent it may present Firm A's AIS service to users through its own platform, eg, its website or application, without being in breach of the prohibition in regulation 138. It must be clear to the customer who they are dealing with and that Firm B is acting as agent of Firm A, the principal. This may include, eg, using Firm A's branding within Firm B's application or website. Further,

the agreement for the provision of AIS will be between the customer and Firm A, the principal. We have provided draft guidance on this in Appendix 1.

Q14: Do you agree with our proposed changes to PERG regarding agents? If not, please explain why.

Perimeter guidance on e-commerce platforms

7.8 Question 33A of Chapter 15 of PERG gives guidance on whether the PSRs 2017 apply to e-commerce platforms that collect payments from buyers of goods and services and then remit the funds to the merchants that sell goods and services. We consulted on this guidance in our April 2017 consultation on the implementation of PSD2.

Proposal

7.9 We are now proposing to add an additional example of a type of e-commerce platform that we expect is likely to fall within the scope of the PSRs 2017. Specifically, we propose to clarify that we would generally expect an e-commerce platform that provides so-called escrow services as a regular occupation or business activity to be offering payment services that are subject to the PSRs 2017, although the individual circumstances of a particular case will always need to be taken into account (see Appendix 1).

Q15: Do you agree with our proposed changes to PERG regarding e-commerce platforms? If not, please explain why.

Closed loop gift cards

7.10 When we originally consulted on implementation of PSD2, we were asked by stakeholders to clarify whether 'closed-loop' gift cards, that do not come under the definition of e-money, were within scope of the limited network exclusion (LNE) and subject to the notification requirements for businesses operating under this exclusion. We acted on this feedback by amending Question 40 of PERG to clarify that excluded instruments under the LNE could include store cards, eg, closed-loop gift cards.

7.11 We have since received feedback that the term has different interpretations and is causing confusion amongst industry participants.

Proposal

7.12 We consider that 'gift cards' are not payment instruments in the way that is intended in PSD2 where the issuer is a retailer and the gift card can only be used to obtain goods or services from that retailer. We propose to make this clarification in PERG (see Appendix 1).

7.13 The outcome of changes to this guidance will be that notifications would not be expected from issuers of gift cards (such as retailers) where the issuer is the only possible beneficiary when the gift card is 'spent'. That includes retailers that issue their own gift cards.

7.14 We propose to remove reference to 'closed loop' and provide further clarification.

Q16: **Do you agree with our proposed changes to PERG regarding closed loop gift cards? If not, please explain why.**

Other changes

7.15 We propose to make the following minor changes to PERG:

- Update 'e-money' in the Handbook to reflect the changes to the electronic communication exclusion and limited network exclusion made by PSD2 (see Appendix 1)

Q17: **Do you agree with these changes to PERG? If not, please explain why.**

Annex 1
Questions in this paper

Q1: Do you agree with our approach to assessing requests for exemption to the contingency mechanism and our related guidance? If not, please explain why.

Q2: Do you agree with our proposal to require quarterly submission to us of the quarterly statistics ASPSPs are required to publish under the SCA-RTS? If not, please explain why.

Q3: Do you agree with our approach to receiving reports about problems with dedicated interfaces? If not, please explain why.

Q4: Do you agree with our changes to the Approach Document to reflect the EBA exemption guidelines, EBA Opinion and the SCA-RTS? If not, please explain why.

Q5: Do you agree with our approach to receiving notifications relating to the fraud rate? If not, please explain why.

Q6: Do you agree with our proposed approach to the corporate payment exemption? If not, please explain why.

Q7: Do you agree with our proposed approach to the application of the strong customer authentication requirements and associated exemptions? If not, please explain why.

Q8: Do you agree with our approach to implementing the EBA fraud reporting guidelines? If not, please explain why.

Q9: Do you have any feedback on how the FCA can best use the data we would receive under the EBA fraud reporting guidelines?

Q10: Do you agree with our proposal to require PSPs and Credit Unions to record and report data on complaints they have received about alleged APP fraud in general? If not, please explain why.

Q11: Do you agree with our proposed Approach Document text clarifying our expectations in relation to PSPs' requirements where the wrong unique identifiers are used? If not, please explain why.

Q12: **Do you agree with our proposed Approach Document text clarifying guidance in light of the contingent reimbursement code developments? If not, please explain why.**

Q13: **Do you agree with our other changes to the Approach Document? If not, please explain why. Please provide section references in your response.**

Q14: **Do you agree with our proposed changes to PERG regarding agents? If not, please explain why.**

Q15: **Do you agree with our proposed changes to PERG regarding e-commerce platforms? If not, please explain why.**

Q16: **Do you agree with our proposed changes to PERG regarding closed loop gift cards? If not, please explain why.**

Q17: **Do you agree with these changes to PERG? If not, please explain why.**

Q18: **Do you agree with the cost and benefits we have identified? If not, please explain why.**

Annex 2
Cost benefit analysis

Introduction

1. The Financial Services and Markets Act (FSMA), as amended by the Financial Services Act 2012, requires us to publish a cost benefit analysis (CBA) of any rules we propose under FSMA. Specifically, section 138I requires us to publish a CBA of proposed rules, defined as 'an analysis of the costs, together with an analysis of the benefits that will arise if the proposed rules are made'. It also requires us to include estimates of the costs and benefits, unless they cannot reasonably be estimated or it is not reasonably practicable to produce an estimate. This requirement to produce a CBA for rules made under FSMA does not apply in specified instances, including where the proposed rules would result in no or only a minimal increase in costs for businesses.

2. Some of the changes we propose will be made under FSMA, such as proposed changes to the Dispute Resolution: Complaints sourcebook (DISP) on complaints reporting. The changes made under FSMA will be subject to our FSMA CBA obligation unless an exemption applies.

3. However, most of the changes in this CP will be made under powers given to us in the PSRs 2017:

- our proposals for guidance in the revised Approach Document and PERG will be made under regulation 120 of the PSRs 2017
- the majority of our proposals for reporting and notifications will be made using our powers to impose reporting requirements under regulation 109 of the PSRs 2017, or various powers to specify the form and content of notifications

4. We are not required to publish a CBA in relation to the exercise of our powers under the PSRs 2017, as drafted. However, regulation 106 (3) of the PSRs 2017 states that we must have regard to (among other things) the principle that a burden or restriction which is imposed on a person, or on the carrying on of an activity, should be proportionate to the benefits. To assist us in assessing the proportionality of our proposals, we have considered whether they impose costs on payment service providers (PSPs) beyond those which are inherent in the PSRs 2017 and related legislation, such as European Commission delegated regulations developed by the European Banking Authority (EBA).

Overall cost of PSD2 implementation

5. We recognise that businesses will incur material costs complying with PSD2. The broader costs have been considered by the European Commission, the UK Government and the European Banking Authority:

- The European Commission carried out an impact assessment, which it published with its directive proposal in July 2013.

- The Treasury has published its own draft impact assessment for its proposed implementation approach. The Treasury has stated that its approach is to copy out PSD2's provisions where possible in creating the PSRs 2017, but to keep using the Member State derogations exercised in the implementation of PSD, to ensure the payment services regime remains, as far as possible, tailored for the UK payments market. The European Banking Authority has published a cost benefit analysis and impact assessment for its development of the Regulatory Technical Standards on strong customer authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2) (SCA-RTS).

6. We have taken the European Commission, the Treasury's and the European Banking Authority's respective impact assessments into account and so have not repeated the analysis presented there in this CBA.

Our implementation approach

7. The proposals in this paper are designed to make sure the aims of PSD2 and related technical standards and guidelines are realised in the UK, and that we are able to effectively monitor and enforce compliance with the PSRs 2017 and related rules.

8. We also seek to advance our statutory objectives, in particular ensuring an appropriate level of consumer protection and promoting effective competition in the interests of consumers.

9. The amendments to our rules (eg, in the Supervision Manual and DISP) are intended to ensure that our Handbook is compatible with the PSRs 2017.

10. We have also significantly revised our Approach Document. The revised Approach Document aims to help PSPs understand their regulatory obligations, particularly those additional requirements which apply from 14 September 2019. It does not impose new or additional obligations.

Summary of our analysis

11. We are providing a separate CBA for each proposal, alongside a summary of the analysis, below. We have not quantified costs where we have only carried out a high-level CBA because we are not adding costs beyond what is required in PSD2. We do not provide a summary of the benefits in the table below, as we have not quantified benefits; instead we provide a qualitative analysis of benefits within each respective CBA.

12. In estimating the number of businesses affected by each proposal, we have generally used the total potential population, based on the regulatory permissions that businesses have. This is likely in many cases to overestimate the actual number of firms affected.

Summary of the CBA

	Proposal	Type of business affected	Estimated number of businesses effected	Estimated cost per business	Total costs
1	Contingency mechanism exemption request	ASPSPs	1092	No significant additional cost imposed above EU obligations	No significant additional cost imposed above EU obligations
2	Reporting of quarterly statistics on performance and availability	ASPSPs	1092	Negligible	Negligible
3(a)	Notification of problems with dedicated interfaces	ASPSPs, AISPs, PISPs and CBPIIs	ASPSPs:1092 AISPs, PISPs and CBPIIs: around 80[2]	No significant additional cost imposed above EU obligations	No significant additional cost imposed above EU obligations
3(b)	Notification when fraud rate is exceeded	PSPs	1557	No additional cost imposed above EU obligations	No additional cost imposed above EU obligations
4	SCA exemption for corporate payments	PSPs	1557	Costs of minimal significance above EU obligations	Costs of minimal significance above EU obligations
5	Fraud reporting	PSPs	1557	No significant additional cost imposed above EU obligations	No significant additional cost imposed above EU obligations
6	APP fraud complaints reporting	PSPs and Credit Unions	1557 PSPs and 475 Credit Unions	See text	£70,000 per year ongoing and £95,000 one-off
7	Minor or consequential changes to the handbook	PSPs	1557	Negligible	Negligible
8	Approach Document	PSPs	1557	Negligible	Negligible
9	Familiarisation costs with all of the proposals	PSPs and Credit Unions	1557 and 475 Credit Unions	See text	£645,000

2 Based on numbers of AISPs and PISPs authorised or pending authorisation as at date of publication

Proposed Handbook changes and directions

1. Contingency mechanism exemption request

Proposals

13. The SCA-RTS will allow competent authorities to exempt providers that are building dedicated interfaces to comply with SCA-RTS requirements, from having to build a 'contingency mechanism' which would be the 'fall-back' access if the dedicated interface failed. ASPSPs must have been granted this exemption in advance of 14 September 2019, or they will have to build the contingency mechanism.

14. While draft EBA exemption guidelines describe the criteria ASPSPs need to meet to be granted an exemption, they do not specify how information to evidence compliance should be provided to competent authorities or what exactly the information should be in all cases.

15. The SCA-RTS and the EBA exemption guidelines are intended to introduce a common approach across the EU. We have little discretion around their implementation. However, the requirements for requesting the exemption are not set out in detail in the RTS. This is why the EBA has consulted on its own guidelines to assist competent authorities in their approach to exempting firms. The EBA exemption guidelines set out the requirements and criteria ASPSPs should meet. However, they do not set out exactly what information competent authorities should request to be satisfied that the requirements and criteria are met.

16. We propose to specify the form, timing and content of requests for exemptions under the SCA-RTS contingency mechanism requirements. Our changes will not add significant additional obligations beyond what is required under PSD2, the SCA-RTS and the guidelines.

Costs

17. Businesses preparing and submitting exemption requests may incur one off costs of familiarising themselves with our guidance. There will also be costs associated with gathering together the necessary information we propose to request (such as whether SCA-RTS requirements are met by the design and implementation of their API and details of the customer journey). Those ASPSPs that have been subject to the CMA order to develop APIs and engaged in the work of the Open Banking Implementation Entity should have this information to hand and costs should be minimal. Other ASPSPs may need to undertake more detailed analysis. However, we have kept the amount of information we ask for to a minimum based mainly on the EBA exemption guidelines.

Benefits

18. We have engaged with ASPSPs that will be seeking the exemption from the contingency mechanism. These ASPSPs have been keen that the FCA provides additional clarity beyond what is set out in the EBA exemption guidelines. In doing so, we believe our proposals will reduce overall costs for ASPSPs by reducing uncertainty and helping with ASPSPs' investment decisions relating to their interfaces for SCA-RTS compliance. This may prevent ASPSPs from having to invest in the contingency mechanism because they will have more confidence in obtaining an exemption.

2. Reporting of quarterly statistics on performance and availability

Proposals

19. Under the SCA-RTS, ASPSPs are required to publish quarterly statistics on the availability and performance of their dedicated interfaces and, for comparison purposes, the interfaces used by their payment service users.

20. We propose directions in SUP to require ASPSPs to submit the quarterly statistics to us quarterly (see Appendix 1).

21. We think there will be negligible additional costs based on us requiring the reporting through our systems. This will allow the benefits envisaged by the SCA-RTS (namely that competent authorities can monitor the performance of interfaces) to be realised.

3(a&b). Notifications under the SCA-RTS

Proposals

22. Under the SCA-RTS, different firms are required to notify in different circumstances: ASPSPs and third-party providers (TPPs) will need to report problems with dedicated interfaces to the FCA; and PSPs must monitor their fraud rate and notify the FCA where the reference fraud rate is exceeded.

23. To receive and record these notifications in a consistent manner, we are proposing directions in SUP. This will include specifying a form, which firms will need to use to submit notifications. The proposed notification forms and draft direction can be found in Appendix 1.

24. We believe our approach does not add significant incremental costs to PSPs beyond the costs imposed by the SCA-RTS.

Costs

25. Businesses may incur one off costs for developing processes and training staff to capture the information which will be required by the SCA-RTS in the way we specify. We have broken the notification forms down into parts and provided options to choose from where relevant. This should make the forms easier to complete and enable us to collect the information in a standardised manner across all notifying businesses. Because our directions and the reporting form is relatively short and accompanied by guidance in our Approach Document, the costs of firms familiarising themselves with the requirements should be minimal.

Benefits

26. Submission of these notifications will be required under the SCA-RTS so we are helping firms to meet their regulatory obligations. Giving firms a standardised way of submitting the information will ensure consistency in the reporting we receive.

4. SCA-RTS exemption for corporate payments

Proposals

27. Under the SCA-RTS, 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 PDS2.

28. We considered developing a new process and form for firms to use to provide us with the information we need to satisfy ourselves that a PSP meets the conditions to apply the exemption. However, instead we propose to clarify that the information we need to be satisfied should be included in the existing operational and security risk assessment annual submission. This information will need to be provided, from 14 September 2019, whenever the operational and security risk form is due to be submitted.

29. We believe our approach is likely to impose only costs of minimal significance to PSPs beyond the costs imposed by PSD2, the SCA-RTS and the existing operational and security risk assessment requirement.

5. Fraud reporting

Proposals

30. Under PSD2, PSPs must report statistical data on fraud relating to different types of payment to the FCA, and we must onward report to the EBA and ECB. However, PSD2 does not specify the form in which the data should be reported. Before the deadline to implement PSD2 (13 January 2018), we consulted on and introduced interim measures to collect fraud data (REP017).

31. The EBA then started work on guidelines to harmonise fraud reporting across the EU. We propose changes to SUP 16 to direct PSPs to submit a new fraud reporting form replacing REP017 now that the EBA Guidelines on fraud reporting under the Payment Services Directive[3] (EBA fraud reporting guidelines) are final. These guidelines are addressed at both competent authorities and PSPs, both of which must make every effort to comply with the guidelines.

32. We believe our approach does not add significant incremental costs to PSPs beyond the costs already imposed by PSD2, the SCA-RTS and the EBA fraud reporting guidelines.

Costs

33. PSPs will need to change systems to submit the new fraud report according to the EBA fraud reporting guidelines. Some PSPs have indicated that current systems do not link fraud reporting to geographic location of the transaction. As the EBA fraud reporting guidelines were finalised in July 2018, we have relatively little time between the publication of the guidance and the need to collect reporting data and therefore we have been unable to collect cost data from firms. One major banking group estimated the latter would have one-off costs of around £2 m. Representatives of PSPs have indicated that the short lead time, due to the EBA's final guidelines being published only recently, will mean transitioning to new reporting will be challenging and costly. Under the approach to fraud reporting we introduced for January 2018 (REP017), all PSPs report fraud statistics annually. Under the EBA fraud reporting guidelines, PSPs will need to report data twice yearly, excluding small PSPs[4] which will need to report annually. The EBA fraud reporting guidelines require these small PSPs nevertheless to provide a 6 month breakdown in their annual report.

3 https://www.eba.europa.eu/-/eba-publishes-final-guidelines-on-fraud-reporting-under-psd2

4 Small payment institutions, small e-money institutions and registered account information service providers

34. The EBA guidelines omit data collection relating to newly regulated account information service providers (AISP). These providers are legally in scope of the reporting, as they are caught by the definition of payment service provider, but they were not included in the guidelines because they are not involved in payment transactions. We are currently collecting AISP fraud data because we are interested in any fraud trends associated with this type of provider and harms relating to data. We propose to continue requiring AISPs to submit fraud data. AISPs will need to meet costs of changing the reporting form (as we migrate to a new reporting form for all PSPs). However, the additional costs associated with collecting the data will be minimal, as AISPs should already be collecting data.

Benefits

35. Industry figures put losses due to financial fraud at nearly £1 billion in 2017.[5] Implementing the EBA fraud reporting guidelines will enable us to collect more detailed and more frequent fraud data. We will be able to use these data to identify trends and patterns in fraud affecting different payment types. In particular, we will receive data which may help us to understand whether new requirements for strong customer authentication have helped to reduce fraud.

6. APP fraud complaints reporting

Proposals

36. We propose to require PSPs and Credit Unions to record and report data on complaints they have received about alleged APP fraud in general. We propose to add to the Payment Services Complaints Return as illustrated in Appendix 1 and the Credit Union Complaints Return also in Appendix 1. The data collected will serve as an indicator of progress on reducing APP fraud and help to inform our supervisory work. Some of these data may be published by the FCA, making it visible to firms and consumers.

Costs

37. We expect most PSPs affected by our proposals are already subject to DISP, and required to report complaints. We would expect that firms already collect such information and therefore the additional costs for firms will be relatively minor. Credit Unions are already subject to DISP.

38. We anticipate firms will incur costs in gathering, checking and reporting the data. To estimate the ongoing cost of reporting complaints data, we have reviewed previous FCA and FSA cost estimates for previous similar complaints reporting requirements. Based on this review and accounting for inflation since previous estimates, we estimate per-firm ongoing costs of providing complaints data to be around £400 for large firms, £70 for medium-sized firms and £20 for small firms. Over the population of PSPs and Credit Unions affected (estimated to be 57 large firms, 194 medium-sized firms and 1,781 small firms), we therefore estimate total ongoing costs to be around £70,000 per year.

39. We also estimate the cost for firms of conducting a legal review of these proposals given they are a new requirement. It is assumed that 4 legal staff at large firms, 2 legal staff at medium firms, and 1 member of legal staff at small firms will review the legal instrument associated with APP complaints reporting. It is further assumed that each legal staff member can review 50 pages of legal text per day. Finally, using data on salaries from the Willis Towers Watson UK Financial Services survey the hourly legal

5 In 2017, fraud losses on cards totalled £566 m and Losses due to authorised push payment scams totalled £236 m https://www.ukfinance.org.uk/wp-content/uploads/2018/03/UKFinance_2017-annual-fraud-update-FINAL.pdf

staff salary is assumed to be £66 at large firms, £66 at medium firms, and £51 at small firms, including 30% overheads.

40. Using these assumptions, we expect firms to incur one-off legal review costs of around £95,000.

Benefits

41. Our complaints reporting proposals enable the FCA to monitor the level of complaints at individual firms. This will enable high levels of complaints to be identified and supervisory action to be directed to areas where harm may be occurring. This should deliver greater levels of consumer protection from fraud.

42. Any data published on the FCA website will be visible to PSPs, Credit Unions and consumers helping to provide transparency on this issue.

43. It is not reasonably practicable to quantify the benefits of our proposals. This is because without collecting these data we are unable to say where harm may be occurring or how supervisory action may reduce this harm.

7. Minor or consequential changes to the Handbook

44. We propose a number of consequential changes to the Handbook as a result of changes imposed by the implementation of PSD2. These include changes to definitions in the glossary. As these changes simply reflect PSD2, we do not believe they will result in additional costs for businesses, and so we do not conduct a CBA.

8. Approach Document

45. We amend or add new guidance to the Approach Document to reflect regulatory technical standards and guidelines under PSD2 which have been finalised since we first published the revised Approach Document in September 2017. PSD2 is a maximum harmonising directive, and we believe that our guidance reflects a reasonable interpretation of PSD2, the PSRs 2017 and related technical standards and guidelines. We do not believe the guidance in the revised Approach Document adds any material cost onto businesses, and so we do not conduct a CBA.

9. Other costs

46. Finally, we estimate familiarisation costs from all the proposals in this CP by assuming that staff in firms affected by PSD2 will read the policy documentation. We anticipate a total of 2,032 firms are affected by the proposals (57 large, 194 medium and 1,781 small). We do not estimate legal review costs for the elements of the proposed new rules that are non-discretionary. We assume that 20 compliance staff at large firms, 5 compliance staff at medium firms, and 2 compliance staff at small firms read the relevant documentation. Using data on salaries from the Willis Towers Watson UK Financial Services survey, the hourly compliance staff salary is assumed to be £57 at large firms, £60 at medium firms, and £42 at small firms. Assuming a reading speed of 100 words per minute, total one-off familiarisation costs are estimated at around £560,000.

47. We also estimate the familiarisation costs arising from the APP fraud complaints reporting for Credit Unions. 475 Credit Unions will be affected (1 medium and 474 small). Using the same assumptions as above but for the relevant policy documentation for Credit Unions, we estimate total one-off familiarisation costs of £85,000.

Q18: **Do you agree with the cost and benefits we have identified? If not, please explain why.**

Annex 3
Proposed Approach Document additions and amendments

Annex 3
Proposed amendments to the Approach Document

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

Changes to the following chapters:

Preface

Chapter 1 – Introduction

Chapter 3 – Authorisations and registration

Chapter 6 - Passporting

Chapter 8 – Conduct of Business requirements

Chapter 13 – Reporting and notifications

Chapter 17 – Payment initiation and account information services and confirmation of availability of funds

Chapter 18 – Operational and security risks

New chapter:

Chapter 20 – Authentication

[please note: new text is underlined; and deleted text is struck through]

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, we merged our Approach Documents on the PSRs and the EMRs ~~Approach Document has been updated throughout~~ to reflect changes brought about by the introduction of the revised Payment Services Directive (PSD2)[2], other changes in the market since our original guidance was issued and as a response to feedback received to our Call for Input (published in February 2016) and to CPs 17/11 and ~~CP~~ 17/22 ~~(published in April and July 2017 respectively).~~

In July 2018, we published a second version of the Payment Services and Electronic Money Approach Document to incorporate new guidance on operational and security risk under PSD2 and other minor amendments[3].

We have updated this latest version of our Approach Document to reflect:

- the finalisation of European rules on passporting and home-host supervision
- the finalisation of European rules 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.
~~the following:~~
~~changes brought about by the introduction of the revised Payment Services Directive (PSD2)~~[4]

[1] As amended by the Payment Systems and Services and Electronic Money (Miscellaneous Amendments) Regulations 2017, available at www.legislation.gov.uk/uksi/2017/1173/contents/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] We consulted on the proposed changes in CP 18/6 (published in March 2018)

~~changes in the market that have an impact on the guidance we first published in 2009 and 2011 respectively~~

~~the feedback received in the course of the Call for Input we published in February 2016~~

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

~~feedback received in the course of CP 17/22 (published in July 2017)~~

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

~~We have merged our Approach Documents on the PSRs 2017 and the EMRs as an outcome of the Call for Input.~~[5]

1. Introduction

[Excerpts for consultation]

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[6].

[…..]

[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.7 The exercise of passporting rights is amended through the PSRs 2017 as well as the EBA Regulatory Technical Standards on passporting under PSD2[8]. 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.

[6] http://www.eba.europa.eu/single-rule-book-qa
[7] 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.
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R2055&from=SL

- 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.

- 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, banks and building societies need to comply with the Banking: Conduct of Business 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 EBA Regulatory Technical Standards on strong customer authentication and common and secure communication (SCA-RTS). See **Chapter 17 – Payment initiation and account information services and confirmation of availability of funds** and **Chapter 20 – Authentication** for further information.

[…..]

Implementation dates and transitional provisions

[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.~~

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 ~~account information services (~~AIS~~)~~ or ~~payment initiation services (~~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** 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. ~~Similarly, to small PIS, T~~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. For UK businesses ~~T~~this includes payment services that are unrelated to the issuance of e-money, ~~.~~

~~h~~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 services 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 includes information about PIs, RAISPs and EMIs and~~,~~ their agents and the ~~ir~~ EEA branches of PIs and EMIs~~, and RAISPs~~. 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.

~~3.11 Applicants that wish to operate through agents will be charged an additional application fee.~~

3.12 Our commitment[9] 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.

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

- 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.
- 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.

Information to be provided and EBA Guidelines

3.123.13The 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 The EBA Guidelines specify the information that applicants for authorisation as a PI or an EMI or registration as a RAISP will be required 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 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.

3.133.14Where 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.

3.143.15As 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. We would expect applicants to fully answer questions in the application form, which includes providing the information requested for in bullets under each question. This information can be

provided in the form, or, as long as it is clearly signposted in the form, in the supporting policy document.

3.153.16 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 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 nothave all the information we need), we will ask in writing for more information. We willconfirm the date when we consider the application to be complete. The timings set outin Part IV: Decision-making process will run from that date.~~

3.163.17 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)

3.173.18 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 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. ~~Where an application is incomplete, applicants will need to provide information promptly to avoid delay to consideration of their application (see 'Timing' in Part IV of this chapter).~~

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

3.183.19 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.

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

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

Part I: Becoming an authorised PI or authorised EMI

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

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

3.23 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.

3.24 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**).

3.25 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

3.26 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).

3.27 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)

3.28 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.

3.29 In both cases, Guideline 3 requires the programme of operations to be provided by the applicant to contain a description of the payment services envisaged, including an

explanation 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.

3.30 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.

3.31 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 and draft contracts between them, and ~~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.

3.32 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)

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

3.34 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.

3.35 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 supervise it or its financial soundness, we can require the applicant to form a separate legal entity to provide payment services and, for EMIs, issue e-money.

3.36 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~~3.37 Applicants wishing to become authorised EMIs that intend to provide unrelated payment services are required to submit a separate business plan for these activities.

~~3.37~~3.38 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)

~~3.38~~3.39 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.

~~3.39~~3.40 The information must include a description of the applicant's relevant outsourcing arrangements (if any). Draft contracts with parties to whom operational functions are outsourced should be provided (see section 18.9 below 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

~~3.40 We will take these factors into consideration when assessing an authorisation application where the business intends to outsource important operational functions.~~

3.41 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.

3.42 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,

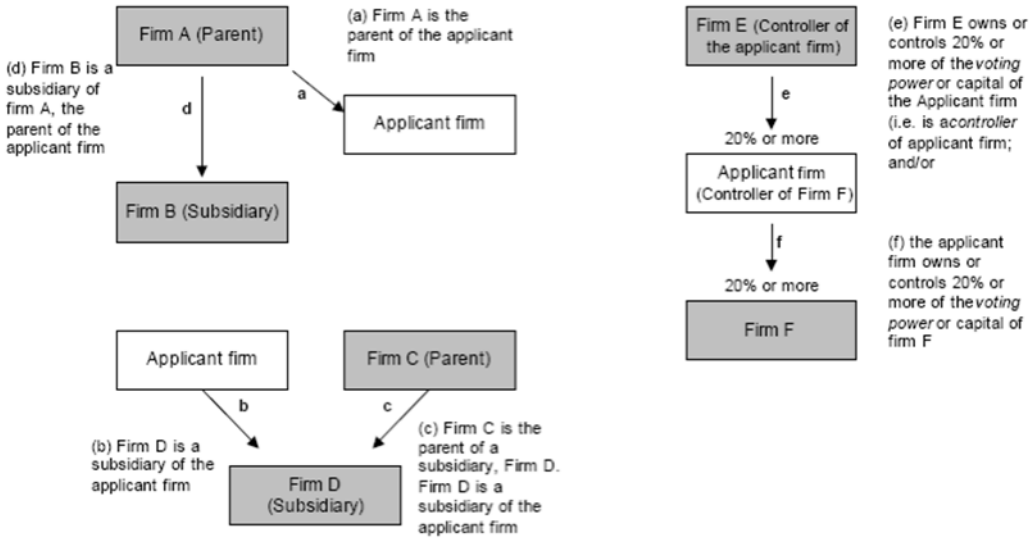
the laws of the foreign territory would not prevent effective supervision (in accordance with regulation 6(9) and (10) of the PSRs 2017 and regulation 6(8) and (9) of the EMRs).

3.43 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

3.44 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.

3.45 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)

3.46 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.

3.47 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.

3.48 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 in Schedule 1 Part 1(1)(a) to (1)(e) to the PSRs 2017.	€125,000

3.49 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

3.50 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 office (and, where relevant, its registered office) is in the UK.

3.51 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

3.52 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)

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

3.54 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)

3.55 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.

3.56 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.

3.57 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

3.58 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.

3.59 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**).

3.60 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).

3.61 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)

~~3.61~~3.62 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.

~~3.62~~3.63 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

~~3.63~~3.64 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~~

~~3.64 API Guideline 8 and EMI Guideline 8 set out the information and documentation that needs to be provided for governance arrangements and internal controls.~~

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

3.66 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)

3.67 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.

3.68 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.

3.69 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)

3.70 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 and EBA Guidelines on major incident reporting[10].

3.71 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**.

[10] http://www.eba.europa.eu/documents/10180/1914076/Guidelines+on+incident+reporting+under+PSD2+%28EBA-GL-2017-10%29.pdf/3902c3db-c86d-40b7-b875-dd50eec87657

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

3.72 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.

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

3.73 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.

3.74 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)

3.75 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**).

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

~~3.76~~ 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.

~~3.77~~3.76 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).[11]

~~3.78~~3.77 More information on security can be found in **Chapter 18 – Operational and security risks.**

[11] https://www.cyberaware.gov.uk/cyberessentials/

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

~~3.79~~3.78 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).

~~3.80~~3.79 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.

~~3.81~~3.80 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 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 counterterrorism obligations is clearly allocated (see also Governance arrangements and risk management controls at paragraph 3.159).

~~3.82~~3.81 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
- 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

~~3.83~~3.82 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.

~~3.84~~3.83 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)

~~3.85~~3.84Applicants that are required to be registered with Her 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 payment service providers ~~PSPs~~
- ~~•~~ telecommunications~~,~~ digital and IT PSPs

~~3.86~~3.85Firms that are already MLR-registered with HMRC should supply their registration number when applying to us. If an application to HMRC is being made at the same time as an application for authorisation, then ~~we will still process the application, but cannot grant authorisation until the MLR registration number has been received~~the applicant should provide their application number.

~~3.87~~3.86We will verify with HMRC that the registration or application number provided to us matches a valid MLR registration or application for that firm.

~~3.88~~3.87Where 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)

~~3.89~~3.88A condition for authorisation under both the PSRs 2017 and EMRs is that the applicant must satisfy us that any persons having a qualifying holding in it are fit and proper persons having regard to the need to ensure the sound and prudent conduct of the affairs of the 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

~~3.90~~3.89A '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'.

~~3.91~~3.90A 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.

~~3.92~~3.91 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.

~~3.93~~3.92 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 applicant~~tion~~ must ~~contain~~ provide ~~the following information~~:

- ~~•~~ information relating to the ~~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)

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

3.93 The relevant forms for providing this information 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.

Assessment of suitability of controllers

3.94 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.

3.95 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 proper~~riety~~',

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).

For more detail on our assessment of controllers' fitness and propriety, see section 3.101 'Assessing fitness and propriety'.

~~3.96 Whilst it is impossible to list every fact or matter that would be relevant to the fitness and propriety of a controller, the following are examples of factors that we will consider. Whether:~~

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

~~3.97 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)

~~3.98~~3.96 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.

~~3.99~~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 ~~Qualifying Holding and~~ 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.

~~and similarly to Qualifying Holdings (controllers), we will assess whether that individual is 'fit and proper'.~~

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

~~3.100~~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
- person(s) 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.

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

3.99 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 ~~reputation~~ 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, ~~and~~ 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).[12] ~~**We attach considerable importance to the completeness and accuracy of the Qualifying Holding and PSD/EMD Individual forms or EMD Individual form. If the applicant is in any doubt as to whether or not any information is relevant, it should be included.**~~

~~3.102~~3.100

~~3.103~~3.101 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.

~~3.104~~3.102 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~~ controller or individual.

Honesty, integrity and reputation

~~3.105~~3.103 In determining the honesty, integrity and reputation of a controller or an individual, the following are examples of factors that we will consider. Whether:~~the matters that we will have regard to include, but are not limited to:~~

- 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;

[12] 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 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;
- 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.
- ~~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;

~~3.106~~3.104 We will consider matters that may have arisen in the UK or elsewhere.

~~3.107~~3.105 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.

~~3.108~~3.106 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.

~~3.109~~3.107 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

~~3.110~~3.108 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)

3.109 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)

~~3.111~~3.110 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 above.

~~3.112~~3.111 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 nonexecutive committee in a one-tier structure)

~~3.113~~3.112 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

~~3.114~~3.113 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.

~~3.115~~3.114 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.

~~3.116~~3.115 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

~~3.117~~3.116 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.

~~3.118~~3.117 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

~~3.119~~3.118 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

~~3.120~~3.119 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.

~~3.121~~3.120 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.

~~3.122~~3.121 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.[13]

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

~~3.123~~3.122 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

~~3.124~~3.123 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.

~~3.125~~3.124 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

~~3.126~~3.125 Where the applicant is a partnership, an unincorporated association or a body corporate, it must provide evidence that any persons having a qualifying holding[14] 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.

~~3.127~~3.126 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) and ~~.~~ ~~S~~small PIs will need to submit controller forms for persons with a qualifying holding.

[13] http://ec.europa.eu/budget/contracts_grants/info_contracts/inforeuro/index_en.cfm

[14] 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.

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

~~3.128~~3.127 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 3.100).

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

~~3.129~~3.128 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).

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

~~3.130~~3.129 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.

~~3.131~~3.130 Only bodies corporate (e.g. a limited company or Limited Liability Partnership (LLP)) can apply to become a small EMI. ~~If the~~An applicant to become a small PI may be a natural person, in which case their place of residence must be in the UK.

~~3.132~~3.131 The location of the head office, registered office and principal place of business is to be supplied as part of the contact details. In assessing the location of the head office we will take the approach set out in section 3.50– 3.54 above. ~~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: 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 dayto- day basis; and 2. the central administrative functions of the firm (e.g. central compliance, internal audit). 3.135~~

~~3.133 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.~~

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

~~3.134~~3.132 The applicant must comply with the registration requirements of the MLRs, where those requirements apply to it (see 3.86-3.89 in Part I above for more on MLR registration requirements).

~~3.135~~3.133 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.

~~3.136~~3.134 Applicants are required to provide a description of the anti-money laundering policies, procedures and controls in place ~~and in any event, the regulatory requirements are the same as those for an authorised PI or authorised EMI as set out in Part I above~~.

Programme of operations

~~3.137~~3.135 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

~~3.138~~3.136 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 ~~and our Handbook.~~ see **Chapter 13 – Reporting and notifications** for more information on the incident reporting requirements.

~~3.139~~3.137 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**.

3.138 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

~~3.140~~3.139 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

~~3.141~~3.140 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

~~3.142~~3.141 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).[15] 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 includes the physical security of applicants' premises.

~~3.143~~3.142 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

~~3.144~~3.143 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).

~~3.145~~3.144 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

~~3.146~~3.145 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).

~~3.147~~3.146 There is more information on safeguarding in Chapter 10 – Safeguarding, including guidance on what we would expect to see by way of organisational arrangements.

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

~~3.148~~3.147 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.

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

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

~~3.149~~3.148 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.

~~3.150~~3.149 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.

~~3.151~~3.150 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.

~~3.152~~3.151 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

~~3.153~~3.152 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.

~~3.154~~3.153 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.

~~3.155~~3.154 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.

3.1563.155 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

3.1573.156 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

3.1583.157 Governance arrangements are the procedures used in the decision-making and control of the business that provide its structure, direction and accountability.

3.1593.158 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 3.1214);
- 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

3.1603.159 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).

~~3.161~~ 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.

~~3.162~~

Part III: Becoming a RAISP

~~3.163~~3.160 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.

~~3.164~~3.161 RAISPs may not provide any payment services other than AIS.

~~3.165~~3.162 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.

~~3.166~~3.163 The application must be signed by the person(s) responsible for making the application on behalf of the applicant firm. The appropriate persons(s) depends on the applicant firm's type, as follows:

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

Company with one director	The director
Company with more than one director	Two directors
Limited liability partnership	Two members
Limited partnership	The general partner or partners

Information to be provided and conditions of registration

~~3.167~~3.164 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. 51

~~3.168~~3.165 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). Together, these documents explain the information that must be supplied with the application and the conditions that must be satisfied.

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

~~3.169~~3.166 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).

~~3.170~~3.167 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.

~~3.171~~3.168 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)

~~3.172~~3.169 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 contain a forecast budget calculation for the first 3 years ~~include how the user of customer data fits into the applicant's business model~~.

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

~~3.173~~3.170 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)

~~3.174~~3.171 The governance arrangements, internal controls and risk management requirements for applications as RAISPs are outlined in RAISP Guideline 6. These are similar to those for an authorised PI (see Part I). ~~Governance arrangements are the procedures used in the decision-making and control of the business that provide its structure, direction and accountability.~~

~~3.175 The description of the risk management procedures provided in the application should show how the business will effectively identify, manage, monitor and report any risks to which the applicant might be exposed.~~

~~3.176 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) • foreign exchange risk (fluctuations in exchange rates)~~

~~3.177~~3.172 Depending on the nature, ~~and~~ scope~~ale~~ and 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**.

~~3.178 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)

~~3.179~~3.173 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. These are similar to those for an authorised PI (see Part I). ~~see Chapter 11 – Complaint handling for complaints 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.~~

~~3.180 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)

~~3.181~~3.174 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).

~~3.182~~3.175 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. These are similar to those for an authorised PI (see Part I). ~~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.~~

~~3.183 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.~~

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

~~3.184~~3.176 The information that should be provided in a security policy document is set out in RAISP Guideline 10. These are similar to those for an authorised PI (see Part I). ~~The security policy must include a detailed risk assessment in~~ ~~relation 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.~~

~~3.185 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).15~~

~~3.186 More information on security can be found in Chapter 18 – Operational and security risks.~~

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

~~3.187~~3.177 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 nonfinancial interests and information on any other professional activities carried out.

~~3.188~~3.178 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)

~~3.189~~3.179 RAISP Guideline 6 requires that an applicant provides the identity of any auditor that is not a statutory auditor.

~~3.190~~3.180 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)

~~3.191~~3.181 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 3.6~~0~~1.

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

3.182 The applicant must provide the address of its head office. There is no requirement in the PSRs 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, and as above, 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.

Part IV: Decision-making process

~~3.192~~3.183 This section relates to the decision-making process for all applications for authorisation and registration under the PSRs 2017 and the EMRs.

~~3.193~~3.184 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)

~~3.194~~3.185 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~~.~~

~~3.195~~3.186 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.

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

~~3.196~~3.187 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 EMRs)

~~3.197~~3.188 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.

~~3.198~~3.189 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.

~~3.199~~3.190 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 financial soundness, we can require the applicant to form a separate legal entity to issue the e-money and/or perform payment services.

~~3.200~~3.191 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)

~~3.201~~3.192 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.

~~3.202~~3.193 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.

~~3.203~~3.194 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.

~~3.204~~3.195 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)

~~3.205~~3.196 In order to continue providing payment services, 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).

~~3.206~~3.197 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.

~~3.207~~3.198 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.

Authorised PIs and small PIs

~~3.208~~3.199 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.~~

~~3.209~~3.200 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.

~~3.210~~3.201 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).

~~3.211~~3.202 The application for registration under these provisions will be assessed in the normal way.

~~3.212~~3.203 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

~~3.213~~3.204 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.

~~3.214~~3.205 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.

~~3.215~~3.206 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.

~~3.216~~3.207 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.

~~3.217~~3.208 Application forms are available on the payment services section of our website.

~~3.218~~3.209 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

~~3.219~~3.210 Businesses that started providing PIS or AIS on or after 12 January 2016 will need to be authorised to provide these services (or registered, if only providing AIS) by 13 January 2018 to continue providing these services. For existing authorised PIs this means that they will need to have successfully applied for re-authorisation and a variation to add AIS or PIS; for existing authorised EMIs, they 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.

~~3.220~~3.211 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 the Regulatory Technical Standards on strong customer authentication and secure communication (SCA-RTS) apply.[16] This means:

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

~~3.221~~3.212 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. 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).**

Payments through network operators

~~3.222~~3.213 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 reauthorisation 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.

In-flight applications

~~3.223~~3.214 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.

[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.

6. Passporting

[Excerpts for consultation]

[6.2] ~~The European Banking Authority (EBA) has published developed 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).[17] 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, t~~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).

[…..]

Introduction

Authorised PIs

[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, and the same conditions apply as for agents of authorised PIs~~,~~. ~~. The RAISP must provide details of agent(s) as part of its passporting application.~~

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 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 application~~notification~~ 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.

[…..]

Making a passport application

Application ('Notice of intention')

[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.
[…..]

Service passports – not involving an EEA agent or distributor
[6.27] In addition to the general information required in all passport applications (see paragraph 6.152), 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 6.152), 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
[6.31] 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 6.152. 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 6.34~~5~~ 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.[18]

[…..]

[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 201/regulation 34(3)(a) of the EMRs 7, 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.

[…..]

[18] At the time of issuing this Approach Document, the EBA has published draft Regulatory Technical Standards on central contact points under PSD2. We will update this document as required
in line with the final standards after they are published in the EU's Official Journal.

Supervision of incoming EEA PIs and EMIs

[…..]

[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[19]

[…..]

[19] At the time of issuing this Approach Document, the EBA has published 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.

8. Conduct of business requirements

……Excerpts for consultation….

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.

[…..]

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 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.

[…..]

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

[…..]

[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 applicaton of strong customer authentication.

[…..]

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 we would expect PSPs to cooperate and make reasonable efforts to recover the funds as required under regulation 90 of the PSRs 2017.

[8.297] We are generally supportive of work by industry to facilitate the recovery of funds in other cases involving fraud. Industry efforts to develop a 'contingent reimbursement model' (CRM) would see PSPs enter into a voluntary scheme to help to address cases of customer detriment due to APP fraud. Under this scheme, if a PSP could have taken steps to prevent instances of APP fraud (such as shutting down the accounts of fraudsters, or implementing confirmation of payee), the PSP will help to reimburse the customer. PSPs are under an obligation to comply with legal requirements to deter and detect financial crime as detailed in **Chapter 19 – Financial Crime**.

This section will be inserted after 'Consent for use of personal data (regulation 97)' and before 'Part III: Additional conduct of business requirements for e-money issuers'.

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

[8.325] 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)

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

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

[20] 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

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, European Commission, European Banking Authority (EBA) or European Central Bank (ECB).

13.2 **Chapter 4 - Changes in circumstances of authorisation or registration** covers the notifications that 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 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[21]. 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.

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.

[…..]

Reports required – Operational and Security Risk Report (REP018) – PSD2

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)

[21] 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

Handbook references: SUP 16.13.9 to 16.13.17 and SUP 16.13.18 to 16.13.21

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 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 from strong customer authentication have in place processes and protocols that guarantee at least equivalent levels of security to those provided for by the Payment Services Directive 2 (see SUP 16.13.18).

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 regulatory.reports@fca.org.uk. We would not expect EMIs to submit a 'nil return' to us.

[…..]

[NEW] Report required – Statistics on the availability and performance of a dedicated interface

Required to submit: ASPSPs that opt to provide a dedicated interface under Article 31 of the SCA-RTS
Frequency: Quarterly
Submission date: Within 1 month of every publication on the ASPSP's website of the statistics required to be published under Article 32(4) of the SCA-RTS
Method of submission: TBC
Handbook references: SUP 16.13.22 to 16.13.23

Content and purpose

In this report, the ASPSP is asked to provide the same statistics that it has published on its website under Article 32(4) of the SCA-RTS. 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 contingency measures under Article 33(6) of the SCA-RTS. This includes KPIs 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 their returns electronically. Gabriel can also be used to view a tailored schedule of your reporting requirements.

ASPSPs that are EMIs should send it to us by email to regulatory.reports@fca.org.uk**.**

[…..]

[Amended] Report required – ~~REP017~~ [EBA] Payments Fraud Report

Required to submit: All PSPs (credit institutions, PIs, EMIs, RAISPs)
Frequency: **SPIs, SEMIs and RAISPs report ~~A~~a**nnually, all other PSPs report twice yearly.
Submission date: Within 2~~1~~ 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 if EMI)
Handbook references: SUP 16.13 (Reporting under the Payment Services Regulations), SUP 16 Annex 27E (~~REP017~~ EBA Payments Fraud Report), SUP 16 Annex 27F (Notes on completing ~~REP017~~ EBA 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)[22] which specify the data to be reported to the FCA. We have implemented these Guidelines in the form of the 'EBA 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~~ EBA Payments Fraud Report available **here**, complete it electronically in Excel, and send it to us by email to regulatory.reports@fca.org.uk.

[…..]

Part II: Notifications

[…..]

13.6 A summary of the notification requirements for PSPs and e-money issuers is shown in the tables below.

SCA-RTS

[NEW] Notification required – NOT004 Notification that a fraud rate has been exceeded (Article 20 of the **SCA-RTS)**

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: TBC
Handbook reference: SUP 15.14.29 to 15.14.37 (Notification that a fraud rate has been exceeded (Article 20 of the SCA-RTS), SUP **15 Annex 12** (Form NOT004)

Content and purpose

[22] 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

Article 18 of the SCA-RTS permits payment service providers not to apply strong customer authentication where the payer initiates a remote electronic payment transaction identified by the payment service provider as posing a low level of risk according to the transaction monitoring mechanism referred to in Article 2 and Article 18 of the SCA-RTS. Article 19 of the SCA-RTS requires payment service providers to ensure that the overall fraud rates for transactions executed under the Article 18 exemption are equivalent to or lower than the reference fraud rates indicated in the Annex to the SCA-RTS. Where a fraud rate monitored calculated in compliance with Article 19 of the SCA-RTS exceeds the applicable reference fraud rate, Article 20(1) of the SCA-RTS requires payment service providers to immediately report to the FCA, providing a description of the measures that they intend to adopt to restore compliance with the reference fraud rates.
See also, **Chapter 20** section 20.61 to 20.66 for more information.

Process
PSPs should follow the instructions on the Connect online system to submit their notification electronically.

[…..]

[NEW] Notification required – NOT005 Problems with a dedicated interface (Article 33(3) of the SCA-RTS)

Required to notify: ASPSPs, AISPs and PISPs
When to notify: The ASPSP, AISP or PISP must notify us without undue delay in line with SUP 15.14.38
Method of submission: TBC
Handbook reference: SUP 15.14.38-15.14.39 (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 Article 33(3) of the SCA-RTS, Account information service providers, payment initiation service providers and account servicing payment service providers are required to report problems with dedicated interfaces without undue delay. Please refer to **Chapter 17 section 17.168** for more information.

Process
ASPSPs, PISPs and AISPs should follow the instructions on the Connect online system to submit their notification electronically.

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 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). 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 PISP or AISP in relation to the 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 are the Regulatory Technical Standards on strong customer authentication and common and secure communication (the 'SCA-RTS'). The SCA-RTS ~~has been~~Once is published in the Official Journal of the European Union in the form of ~~, the SCA-RTS will become~~ a Commission Delegated Regulation.[23] The security measures referred to in regulations 68(3)(c), 69(2)(a) and (3)(d), 70(2)(a) and (3)(c), 77(4)(c) and 77(6) and 100 of the PSRs 2017 (secure

[23] 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

communication and authentication) and the associated SCA-RTS will apply to firms from ~~18 months after the SCA-RTS enters into force~~14 September 2019. The European Banking Authority (EBA) issued an Opinion on the implementation of the SCA-RTS (the 'EBA Opinion')[24], which provides clarity on certain requirements. The SCA-RTS and the EBA Opinion ~~, once it becomes a Commission Delegated Regulation,~~ should be read alongside the relevant sections in this chapter. Guidance on the SCA-RTS 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. 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 a description of the applicant's security control and mitigation measures to provide adequate protection to users and how these measures ensure a high level of technical security and data protection, 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. 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~~ nine parts:

- scope of accounts subject to the requirements
- requirements on ASPSPs

[24] 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 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 ~~and CBPIIs~~ 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

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 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 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 17.50 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 SCA-RTS is published in the Official Journal of the European Union~~from 14 September 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 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[25] 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 17.76-17.85.

Confirmation of the availability of funds (regulation 68(4))

17.22 If the ASPSP receives a request that meets the requirements of regulation 68(2) of the PSRs 2017, and in accordance with SCA-RTS Article 36(1)(c), the ASPSP must immediately provide a 'yes' or 'no' answer on the availability of the amount necessary for the execution of the card-based payment transaction. We consider 'immediately' in this context to mean that the response should be sufficiently fast so as not to cause any material delay in the payment transaction, 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 instrument issuer, the ASPSP is required to take into account 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.

[25] 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.

Information about provision of a similar response to PISPs is addressed in section 17.26 – 17.29.

Information on the initiation of the payment transaction (regulation 69(2)(b))

17.24 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.

17.25 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 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' would include information regarding a failure or refusal to execute a transaction.

17.26 SCA-RTS Article 36(1)(c) requires an ASPSP to respond to a request from a PSP with an immediate 'yes' or 'no' confirmation as to whether the amount necessary for execution of a payment transaction is available on the payer's payment account. While regulation 68 of the PSRs 2017 (Article 65 of PSD2) is specific to transactions involving CBPIIs, the EBA Opinion clarifies that provision of the 'yes' or 'no' confirmation also applies to requests received from PISPs to help them manage the risk of non-execution.

17.27 When determining its response to a PISP's 'yes' or 'no' request, the ASPSP should take into account the same information (eg 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 say 'yes' if it would execute a payment instruction given by a customer directly.

17.28 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.

17.29 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. In our view, there is no requirement for the PISP to have additional authorisation or registration as an AISP for this purpose.

Treatment of data requests and payment orders (regulations 69(2)(c) and 70(2)(b))

~~17.27~~17.30 Though they may provide factual information explaining AIS and PIS, ASPSPs must not prohibit or discourage customers from using AIS or PIS (eg by communicating to customers that they will be responsible for unauthorised transactions if they share their personalised security credentials with AISPs and PISPs).

~~17.28~~17.31 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.

~~17.29~~17.32 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 17.59 on sensitive payments data below). The amount of information which is required to be disclosed will, therefore, differ across ASPSPs and across accounts. In line with the EBA Opinion, this should be the maximum amount of information that would be available to the customer if the customer accessed the payment account directly, irrespective of what channel they use to access the AISP (for example a web browser or mobile application). To give some examples, we would expect the following sorts of information to be included where the information is available to the customer directly:

- information relating to the account, such as the name on the account and the account number; and

- transaction data, which should be provided to the same level of granularity and cover the same time periods as is available to the customer when they access their account directly. 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.

17.33 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).

~~17.30~~17.34 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.

17.35 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).

~~17.31~~17.36 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.

~~17.32~~17.37 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/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))

~~17.33~~17.38 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.

~~17.34~~17.39 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 71(7), 71(8))

~~17.35~~17.40 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.

~~17.36~~17.41 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).

~~17.37~~17.42 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.

~~17.38~~17.43 ASPSPs should not deny access to an AISP or PISP solely on the basis that it is a member of a particular category of AISP or PISP. The ASPSP must have an objective justification for, and appropriate evidence to support, a suspicion that fraudulent or unauthorised access by each individual AISP/PISP in that category has occurred or will occur. ASPSPs may, in some circumstances, decide to deny a particular AISP or PISP access only to a specific payment account. 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.

~~17.39~~17.44 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**).

~~17.40~~17.45 The ASPSP must restore access to the AISP or PISP as soon as the reasons for denying access no longer exist.

~~17.41~~17.46 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 17.41). 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

~~17.42~~17.47 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))

~~17.43~~17.48 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 and PISPs' obligations in relation to sensitive payment data (which include personalised security credentials) in paragraphs ~~17.51 – 17.54~~ 17.58 – 17.61.

~~17.44~~17.49 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))

~~17.45~~17.50 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.

~~17.46~~17.51 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 in **Chapter 8 – Conduct of business requirements** for further details regarding data protection law.

~~17.47~~17.52 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 payment account information will be used and whether any other parties will have access to that information. It is the AISP or CBPII's responsibility to ensure that the customer has received sufficient information in order to give explicit consent.

~~17.48~~17.53 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.

~~17.49~~17.54 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, in our view, ~~, nor~~ 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. 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 68(3) (c), 69(3)(d) and 70(3)(c))

~~17.50~~17.55 Regulation 68(3)(c), 69(3)(d) and 70(3)(c) of the PSRs 2017 apply ~~18 months after the SCA-RTS is published in the Official Journal of the European Union~~from 14 September 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 17.86 to 17.92 ~~on Requirements on all ASPSPs for secure communication from 14 September 2019~~). CBPIIs must authenticate themselves towards the ASPSP before each confirmation request. There is no 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.

17.56 SCA-RTS Article 34 requires CBPIIs, PISPs and AISPs to identify themselves towards the ASPSP using qualified certificates issued by Qualified Trust Service Providers.

~~17.51~~17.57 CBPIIs, PISPs and AISPs are also obligated to communicate in accordance with the SCA-RTS. ~~We expect the~~ SCA-RTS Articles 28 to 36 ~~to~~ 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/CBPIIs use, they must be able to meet all of the requirements in the PSRs 2017 and the SCA-RTS (e.g. AISPs must access information only from designated payment accounts). Further guidance on AISPs, PISPs and CBPIIs' obligations before the SCA-RTS apply can be found in paragraphs 17.~~66~~76-17.~~71~~81.

Sensitive payment data (regulations 69(3)(e) and 70(3)(e))

~~17.52~~17.58 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.

~~17.53~~17.59 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.

~~17.54~~17.60 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.

~~17.55~~17.61 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 / PISP. The PISP is not, however, permitted to use sensitive payment data obtained or held for the purposes of the other payment service when it is providing the PIS.

Using, accessing and storing information (regulations 68(8)(a), 69(3)(g) and 70(3)(f))

~~17.56~~17.62 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.

17.63 Under SCA-RTS Article 36(3), ASPSPs 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 for a sub-set of their account data to be accessed, only this should be accessed by the AISP.

~~17.57~~17.64 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.

~~17.58~~17.65 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.

~~17.59~~17.66 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.

~~17.60~~17.67 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.

~~17.61~~17.68 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))

~~17.62~~17.69 A PISP must not hold the payer's funds in connection with the provision of the PIS at any time.

Requesting information (regulations 69(3)(f))

~~17.63~~17.70 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 17.26 above.

Not changing the payment order (regulation 69(3)(h))

~~17.64~~17.71 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))

~~17.65~~17.72 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).

17.73 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

~~17.66~~17.74 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 requirement**s;

- 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**.

~~17.67~~17.75 ASPSPs, CBPIIs, AISPs and PISPs also need to be aware of their obligations under data protection law (see paragraphs 8.52 – 8.59 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

~~17.68~~17.76 In relation to certain provisions, there is a transitional period beginning on 13 January 2018, which will end when ~~and ending 18 months after the date~~ the SCA-RTS enters into effect on 14 September 2019~~force~~. During that transitional period, ASPSPs, CBPIIs, PISPs and AISPs are required to comply with regulations 68, 69 and 70 of the PSRs 2017, except for regulations 68(3)(c), 69(2)(a) and (3)(d), 70(2)(a) and (3)(c),

77(4)(c) and (6) and 100 which depend on the SCA-RTS and start to apply at the same time as the SCA-RTS.

~~17.69~~17.77 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.

~~17.70~~17.78 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 17.40~~34~~ – 17.46~~40~~). 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.

~~17.71~~17.79 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.

~~17.72~~17.80 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.

~~17.73~~17.81 During the period before the SCA-RTS becomes applicable, the parties may find it helpful to take account of standards[26] which are being developed as a result of the Competition and Markets Authority's Open Banking Remedy.[27]

Businesses providing AIS or PIS before 12 January 2016

17.82 We have provided guidance in **Chapter 3 – Authorisation and registratio**n 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.

17.83 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

[26] More information on Open Banking delivery can be found here: https://www.openbanking.org.uk/

[27] 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

AIS. As a result, ASPSPs will not be obligated to allow them access to customers' payment accounts.

~~17.74~~17.84 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.

HM Treasury and FCA Expectations for the third party access provisions in PSD2

~~17.75~~17.85 HM Treasury and the FCA issued a joint communication in July 2017[28] 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.[29]

[.....THE REMAINDER OF THIS CHAPTER IS NEW DRAFT TEXT FOR CONSULTATION.....]

Requirements on all ASPSPs for secure communication

17.86 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'.

17.87 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'

17.88 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.

17.89 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).

28 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

29https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/630135/Expectations_for_the_third_party_access_provisions_in_PSDII.pdf

17.90 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')

17.91 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: identification, secure communication and allowing AISPs and PISPs to rely on all the authentication procedures provided by the ASPSP to the customer.

17.92 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

17.93 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

17.94 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.

17.95 The contingency measures cover:

- having a strategy and plans in place for when its 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

17.96 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 customer's online banking portal. 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.

17.97 Where the contingency mechanism is relied upon, the ASPSP must ensure the customer's online banking portal meets the general obligations for access interfaces (SCA-RTS Article 30). This includes providing a means for the AISP or PISP to be identified (see section 17.56 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

17.98 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).

17.99 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 be met to benefit from an exemption from contingency measures under SCA-RTS Article 33(6) of Regulation (EU) 2018/389 ("the EBA Guidelines").[30].

Requesting exemption from contingency measures under SCA-RTS Article 33(6)

17.100 ASPSPs wishing to request exemption from the contingency mechanism requirement need to complete an exemption request form and submit it to us along with the required information. 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 its permissions into the UK from the EEA should submit its exemption request to its home state regulator, rather than the FCA.

17.101 Where a group of ASPSPs or a single ASPSP operates a number of dedicated interfaces, eg in respect of different banking brands, we require separate requests in respect of each dedicated interface for which an ASPSP is seeking an exemption.

17.102 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.

[Note: This following section is based on the EBA's draft Guidelines on the conditions to be met to benefit from an exemption from contingency measures under SCA-RTS Article 33(6) of Regulation (EU) 2018/389 (SCA-RTS on SCA & CSC)'. It will be updated once the final document is published by the EBA.]

Information to be provided and EBA guidelines

17.103 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.

[30] 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)

17.104 In section 17.107 below we provide guidance on the information we will require from ASPSPs in order to make an assessment of whether the conditions in the SCA-RTS and Guidelines have been met.

Processing exemption requests

17.105 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

17.106 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 decision in writing.

Exemption criteria and FCA information requirements

17.107 In order to assess whether the requirements of the EBA Guidelines are met, we require ASPSPs to provide the information set out in 17.107 – 17.165 using the form specified in *SUP 15C Annex 1*. Each information requirement has a question number (eg **Q1**). We will also ask for supporting evidence, including, where relevant, the results of conformance testing (see section 17.152).

Service level, availability and performance (EBA Guideline 2)

17.108 EBA Guideline 2 concerns the service level, availability and performance of ASPSPs' dedicated interfaces. We require the following information:

Q1 Confirmation that the ASPSP has the same service level objectives and targets, out of hours support, monitoring and contingency plans as it has in place for the interface(s) used by its own customers, as per EBA Guideline 2.1.

Q2 Confirmation that the ASPSP has in place the key performance indicators of availability described in EBA Guideline 2.2 for both its dedicated interface and each of the interfaces used by its customers.

Q3 Confirmation that the ASPSP has in place the key indicators of performance described in EBA Guideline 2.3 for its dedicated interface.

Q4 Confirmation that the key performance indicators are calculated in accordance with EBA Guideline 2.4.

Publication of indicators (EBA Guideline 3)

17.109 EBA Guideline 3 concerns the publication of daily statistics on a quarterly basis on the availability and performance of the dedicated interface and of the interface used by an ASPSP's customers as required under SCA-RTS Article 32(4). We require the following information:

Q5 A plan for publication to be provided to competent authorities. This should include:

- the planned date of the first publication
- a description, including website address if possible, of where the statistics will be published on the ASPSP's website

The FCA encourages ASPSPs to locate these statistics in an accessible location, and in close proximity to webpages covering service metrics required under BCOBS 7 (information on current account services)[31].

Q6 Confirmation that the publication each quarter will present daily statistics on a quarterly basis on availability and performance as set out in Guideline 2.2 and 2.3 of the EBA Guidelines for the dedicated interface and each customer interface together.

Q7 Confirmation that, from the date of first publication, the publication will provide a comparison of the availability of the ASPSP's dedicated interface with its best-performing customer interface.

17.110 ASPSPs should note that we have required the quarterly reporting to the FCA of these quarterly published statistics. 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)

17.111 EBA Guideline 4 concerns stress-testing referred to in SCA-RTS Article 32(2). The EBA Guideline notes that 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 and AISPs, in terms of the impact that such stresses have on the availability and performance of the dedicated interface. Under the EBA Guidelines, adequate stress testing should include, but is not limited to:

a) the capability to support access by multiple firms;
b) the capability of the dedicated interface to deal with unusually high numbers of requests, from PISPs, AISPs and CBPIIs, in a short period of time without failing;
c) the use of an extremely high number of concurrent sessions open at the same time for payment initiation and account information requests; and
d) requests for large volumes of data.

17.112 We are primarily concerned that once in operation with AISPs, PISPs and CBPIIs, the ASPSPs' 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 should 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

[31] https://www.fca.org.uk/publication/policy/ps17-26.pdf

understand and forecast when peak usage or other stresses may occur in order to undertake adequate stress testing.

17.113 In order to assess whether this requirement is met, we require the following information:

Q8 Confirmation that adequate stress testing has been undertaken in accordance with EBA Guideline 4.2 a-d.

Q9 A summary of the result of the stress testing covering points a-d, including any weaknesses or issues identified and confirmation that these have been addressed. As part of this, ASPSPs should inform us whether the views of AISPs, PISPs and CBPIIs, or representatives of these market participants, were sought about likely peak usage periods or other stresses.

Obstacles (EBA Guideline 5)

17.114 EBA Guideline 5 concerns obstacles as described in SCA-RTS Article 32(3). Under Article 32(3) an ASPSP must ensure that its dedicated interface does not create obstacles to the provision of payment initiation and account information services. Under SCA-RTS Article 33(6)(a), the FCA cannot exempt an ASPSP that does not meet this requirement. SCA-RTS Article 32(3) sets out that such obstacles may include, among others:

a) Preventing the use by PSPs referred to in Article 30(1) of the credentials issued by account servicing payment service providers to their customers
b) Imposing redirection to the ASPSP's authentication or other functions
c) Requiring additional authorisations and registrations in addition to those provided for in Articles 11, 14 and 15 of PSD2
d) Requiring additional checks of the consent given by customers to providers of payment initiation and account information services.

17.115 In addition, the EBA notes in the Guidelines that the following would constitute such an obstacle:

e) Imposing on authorised AISPs, PISPS and CBPIIs requirements in addition to those detailed in the legislation where they are not equally applied to credit institutions that provide such services because there should be no discrimination in the treatment of providers.

Our assessment of obstacles

17.116 ASPSPs seeking exemption should develop dedicated interfaces that provide (and do not prevent or frustrate) good experiences for both customers and AISPs, PISPs and CBPIIs. As the EBA Guidelines set out, 'the IT solution for the dedicated interface and its implementation should 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 AISPs or PISPs (EBA Guideline 5.2(d)).

17.117 In order to assess whether an ASPSP's dedicated interface creates obstacles, under EBA Guideline 5, we require an ASPSP to provide the following information:

Q10 A summary of the method(s) of access chosen by the ASPSP

Q11 Where the ASPSP has put in place only one method of access, an explanation of the reasons why this method of access is not an obstacle as referred to in Article 32(3) of the SCA-RTS and how this method of access supports all authentication methods provided by the ASPSP to its customer.

Q12 Confirmation that the interface meets the requirements of EBA Guideline 5.2 a – d.

Q13 A visual representation by ASPSPs of the customer journey when a customer accesses their payment account via PISP or AISP (including any authentication steps that take place in the ASPSP's domain).

Guidance on the information to be provided as part of Q10 - summary of method(s) of access (EBA Guideline 5.1 (a))

17.118 'Methods of access' refers to the ASPSP's procedure for the authentication of the customer where a PISP or an AISP is using an ASPSP's dedicated interface. The EBA's Opinion[32] describes different access methods:

- 'Redirection' / 'decoupled' – a customer's authentication data are exchanged directly between the customer and ASPSP
- 'Embedded' – a customer's authentication data are exchanged between AISP/PISP and ASPSPs through the ASPSP's dedicated interface.

17.119 'Redirection' is described in the EBA Guidelines as 'a process whereby once consent has been given to the AISP/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'.

17.120 The FCA's understanding of 'decoupled' (also known as out-of-band authentication) is that it allows the customer to complete the authentication 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.

17.121 The FCA's understanding of 'embedded' authentication is that it is an access method which 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 where the ASPSP offers the embedded access method.

17.122 The summary of methods of access for **Q10** should describe which access method(s) are enabled by the ASPSPs dedicated interface. It should include a description of the flow of authentication data (credentials) from the customer to the ASPSP and, where relevant, at

[32] EBA Opinion section 48

which point, if at all, the AISP or PISP comes into possession of the authentication data/ credentials.

17.123 ASPSPs may also submit an illustration of the access method(s) provided by the dedicated interface, in order to assist our assessment.

Guidance on information to be provided when one method of access is provided – (EBA Guideline 5.1(b))

17.124 Where the ASPSP has put in place only one method of access we require an explanation of the reasons why this method of access is not an obstacle and supports all authentication methods provided by the ASPSP to its customer. Points a-d in EBA Guideline 5.2 cover possible restrictions or obstructions. The explanation given should consider these points.

17.125 It should be noted, in line with the EBA Opinion, that 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 state that it "may" be so, if the ASPSP implements it in a manner which is restrictive or obstructive for AISPs or PISPs.

Guidance on confirming requirements of EBA Guidelines 5.2 have been met

17.126 Whether or not more than one access method is provided, we require confirmation that the requirements in EBA Guideline 5.2 are met (Q12). These are as follows:

- EBA Guideline 5.2(a) - Reliance on security credentials

17.127 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.

17.128 ASPSPs must 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.[1] 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.

17.129 An explanation should be given in this section where authentication methods that the customer can use when directly accessing their account are not available to the customer accessing their payment account through an AISP or PISP.

17.130 In our view and in line with the EBA Opinion[33], where an interface allows for redirection, an AISP or PISP is not prevented from relying on the ASPSP issued credentials. This is because the AISP or PISP is able to 'use' the customer credentials and rely upon the ASPSP authentication procedures. Furthermore, the AISP or PISP is not required to issue its own credentials or authentication procedures.

- EBA Guideline 5.2(b) - Additional requirements not imposed by legislation

[33] EBA draft guidelines paragraph 34(a)

17.131 EBA Guideline 5.2(b) sets out that PISPs, AISPs and CBPIIs do not have to comply with any different or additional requirements, other than those imposed by legislation, that are not equally imposed on all other types of PSPs. 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 (ie that run by the Open Banking Implementation Entity (OBIE) in the UK). In our view, this is not contrary to EBA Guideline 5.2(b), as long as such enrolment is based on no condition other than FCA registration or authorisation and enrolment applies equally to ASPSPs, AISPs, PISPs and CBPIIs. We consider that enrolment in such initiatives can facilitate stakeholder input and collaboration to help ensure the proper functioning of APIs.

17.132 Where an ASPSP does consider that it imposes requirements that are contrary to EBA Guideline 5.2(b), we require an explanation of what those requirements are and their justification.

- EBA Guideline 5.2(c) - Additional checks of consent

17.133 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, as they constitute an obstacle to the provision of AIS or PIS. 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.

17.134 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.

17.135 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.

17.136 In cases where a customer has more than one account with an ASPSP, the customer will need to choose the account which it wishes to be accessed by the AISP, or the account from which a payment should be executed in the case of a PISP. Where the ASPSP provides a redirection method of access, account selection may be carried out between the customer and the ASPSP. This alone will not amount to an obstacle to the provision of AIS or PIS.

17.137 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.

- EBA Guideline 5.2(d) - Dissuading customers through unnecessary delays or friction

17.138 Under EBA Guideline 5.2(d), the ASPSP should confirm that the IT solution for the dedicated interface and its implementation 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.

17.139 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[34].

17.140 Where particular features of an ASPSP's implementation of the dedicated interface may be considered an obstacle under the SCA-RTS and EBA Guidelines (for example, if those features are mentioned in SCA-RTS Article 32(3)), it should consider providing, as part of its exemption request submission (answer to **Q12)**), the results of research or testing which demonstrates that customers are not dissuaded from using the services of PISPs, AISPs and CBPIIs as a result of any feature of the interface.

Design and testing to the satisfaction of PSPs (EBA Guideline 6)

17.141 Under SCA-RTS Article 33(6)(b), in order to exempt an ASPSP, we must be satisfied that the dedicated interface has been designed and tested in accordance with Article 30(5) to the satisfaction of PSPs that use the testing facility.

17.142 ASPSPs that wish to be exempt before 14 September 2019 need to have made technical specifications and testing facilities available to AISPs, PISPs and CBPIIs no later than 14 March 2019 to qualify for an exemption.

17.143 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.

17.144 In order to assess whether an ASPSP's dedicated interface meets the criteria set out in EBA Guideline 6, we require the following information:

Q14 Confirmation, as per EBA Guideline 6.1(a), that the ASPSP has published a summary of the technical specification 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 will need to meet the requirements of SCA-RTS Article 30(3).

Q15 Confirmation, as per EBA Guideline 6.1(b), that the ASPSP has made available a testing facility for the dedicated interface that allows AISPs, PISPs and CBPIIs to test the dedicated interface in relation to points a-f in Guideline 6.2 and the date from which the testing facility was made available.

[34] To this end, we note that 'app-to-App' redirection standards have been developed by OBIE for implementation under the CMA Order by March 2019.

Q16 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. However, the summary of testing results should:

- Identify which, if any, of point a-f have presented problems when tested with AISPs, PISPs and CBPIIs
- Briefly describe what these problems were and whether they were raised by the ASPSP, or by AISPs, PISPs or CBPIIs
- Briefly describe the steps taken to resolve the problems and whether the problems have been resolved

17.145 Where the results of testing demonstrate that problems raised by AISPs, PISPs and CBPIIs have been resolved, this will be taken into account in our assessment of whether the interface has been designed and tested to the satisfaction of PSPs (also see the section below on satisfaction).

Q17 Details of which initiative standard is being implemented (as per EBA Guideline 6.4(a)).

Q18 Results of conformance testing of the implemented API against an initiative standard, for example, a completed conformance checklist (see guidance below – 17.152).

Q19 Details of whether, and if so how and why, the ASPSP has deviated from any standard implementation requirements of the initiative, if available, as per EBA Guideline 6.4(b) (see guidance below – 17.152).

Q20 Where an ASPSP is not implementing a market initiative standard, a description as to the form of engagement that has taken place with PISPs, AISPs and CBPIIs for implementing the dedicated interface as per Guideline 6.5 (see guidance below – 17.152).

Q21 Where an ASPSP is not implementing a market initiative standard, a completed PSD2 checklist based on the EBA Opinion 'Table 1 – Main requirements for dedicated interfaces and API initiatives'.

17.146 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 6.2 and Article 33(6)(b) of the SCA-RTS.

Testing certificates (EBA Guideline 6.2(b))

~~17.76~~17.147 Under EBA Guideline 6.2(b), ASPSPs must make facilities available that enable AISPs and PISPs to test the ability to exchange qualified certificates for electronic seals and qualified web authentication 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, it will be enough for the ASPSP to replicate the functionality of such certificates for the purpose of this testing, as opposed to using certificates actually issued by Qualified Trust Service Providers.

Guidance on the information to provide relating to conformance testing and standard implementation requirements (under EBA Guideline 6.4)

17.148 In paragraph 48 of its consultation document on exemption conditions[35], the EBA sets out its view that the reference to 'design' in the SCA-RTS (Article 33(6)(b)) relates to the legal requirements for access and data detailed in PSD2 and the SCA-RTS. The EBA also notes (paragraphs 49-50) that competent authorities should identify whether different types of market participants have been involved and may also consider the work undertaken by other organisations when considering the design of the dedicated interface.

17.149 We expect that in the development of their 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.

~~17.77~~17.150 We note that as part of their work initiatives[36] such as the OBIE will facilitate conformance testing (also known as compliance testing) of dedicated interfaces against their specified API standards as well as against PSD2 legal requirements.

17.151 As well as testing that standards and legal requirements are met, conformance testing of implemented APIs may cover other aspects which are relevant to ASPSPs' obligations under PSD2, the SCA-RTS and EBA Guidelines exemption conditions. This can include assessing the overall customer journey when dedicated interfaces are used (relevant to the assessment of obstacles) and monitoring overall performance of the dedicated interface (relevant to the assessment of service levels and availability).

17.152 As such, in assessing whether a dedicated interface has been designed and tested to the satisfaction of PSPs, we will make use of the results of conformance testing undertaken by initiatives such as the OBIE.

Submitting standard implementation requirement checklists (Q18)

17.153 EBA Guideline 6.4 refers to the standards against which ASPSPs will undertake conformance testing as 'standard implementation requirements'. We are aware that market initiatives will be recording the results of conformance testing for individual ASPSPs using standard implementation requirement checklists.

17.154 ASPSPs that have undertaken conformance testing should provide the result in the form of the completed standard implementation requirement checklist, or, where a checklist is not provided by the initiative, in the form in which the ASPSP is provided with the results of conformance testing.

[35] 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)

[36] 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

17.155 Where an ASPSP seeking an exemption confirms that its interface follows the standard implementation requirements of a market initiative and provides the results of conformance testing, this will provide a level of assurance that the ASPSP meets the requirements of Article 33(6)(b).

17.156 Conversely, where there is deviation from a market initiative's standard implementation requirements, we will require additional information to enable us to consider more closely whether such deviation is nonetheless compliant with the PSD2 requirements.

Providing information about deviation from standard implementation requirements (SIR) (Q19)

17.157 As per EBA Guideline 6.4, an ASPSP must confirm whether, and if so how and why, it has deviated from any SIRs of the initiative, if available. Where an ASPSP has deviated, its explanation should cover the following:

- Which SIR(s) there is a deviation from
- How the implemented API departs from the SIR(s)
- The justification for the departure. This could cover, for example, whether AISPs, PISPs, CBPIIs and, where appropriate, customers have been consulted about the departure, or whether the departure is due to a different legal interpretation of the PSD2 requirements.

ASPSPs not implementing a market initiative standard (Q20 - 21)

17.158 As per EBA Guideline 6.5, where an ASPSP is not implementing a market initiative standard, we require the ASPSP to provide a description as to the form of engagement that has taken place with PISPs, AISPs and CBPIIs for implementing the dedicated interface. This description should cover the following:

- Which market participants have been involved in the design and testing of the dedicated interface
- What steps have been taken to involve market participants and take on their feedback (i.e. consultations, meetings, roundtables, sandbox testing)
- What steps have been taken to ensure alignment between the API and PSD2 requirements

17.159 Given such an ASPSP will not have been through a market initiative's conformance process, we will require additional information to enable us to consider more closely whether such implementations are compliant with the PSD2 legal requirements for access and data discussed above. We will require these ASPSPs to complete and submit a checklist based on the "main requirements for dedicated interfaces and API initiatives table" which can be found in the EBA Opinion (and is included in the form to be completed for an exemption request).

Wide usage of the interface (EBA Guideline 7)

17.160 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.

17.161 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:

Q22 The number of PISPs, CBPIIs, AISPs and PSPs (including those not yet authorised that have applied for the relevant authorisation) that have made use of the testing facility

Q23 The number of AISPs, PISPs and CBPIIs that are using the interface. In our view, use of the interface means that ASPSPs will have enabled AISPs, PISPs and CBPIIs to use their API interface to provide their services in a live environment to their customers for 3 months.

17.162 The EBA Guidelines acknowledge that not all ASPSPs will be able to demonstrate wide usage of their API 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. We would note that the results of conformance testing can help to demonstrate that an ASPSPs 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.

17.163 Where it has not been practically possible to evidence fulfilment with the condition of 'widely used' set out in EBA Guideline 7.1 for aspects of an interface, we may use the availability of testing facilities as a proxy for wide usage. As part of this, we will require the ASPSP to provide the following information:

Q24 Which aspects of the interface have been used by AISPs, PISPs, or CBPIIs

Q25 A description of the measures undertaken to ensure that the availability of the testing facilities for these aspects has been well publicised via appropriate channels, including where appropriate the website of the ASPSP, social media, industry trade bodies, conferences and direct engagement with known market actors. We expect the ASPSP to demonstrate that at least 3 months of communication of the testing facilities has taken place.

17.164 As per EBA Guideline 7.2, wide usage can be demonstrated concurrently with the testing period. This means that where the ASPSP is meeting its requirement to test 6-months in advance of 14 September 2019 having started to test on 14 March, 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)

17.165 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:

Q26 A description of systems or procedures in place for tracking, resolving and closing problems, including those reported by PISPs, AISPs and CBPIIs. This

should include describing out of hours support, service level objectives for problems resolution and ticketing systems for issues raised.

Q27 Confirmation that the service level for dedicated interface problem resolution is equivalent to the service level for resolving problems with the interface used by the ASPSP's own customers (as per EBA Guideline 2.1). This should include an outline of what the service level targets are for each.

Q28 As per EBA Guideline 8.1(b), an explanation of the problems that have not been resolved without undue delay in accordance with the service level targets and support detailed in EBA Guideline 2.1. In our view, for the purposes of the exemption, the explanation should focus on problems raised during functional testing under SCA-RTS Article 30(5) and the areas for testing identified in EBA Guideline 6.2 points a-f. ASPSPs should inform us of the number of reported problems from these categories that have breached its service level targets for problems resolution, and breakdown this number into the a-f categories. ASPSPs should also include a description of problems reported during operational use of the dedicated interface.

Revoking exemptions

17.166 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).

17.167 As noted in section 17.97, where the contingency mechanism is relied upon the ASPSP must ensure the customer's online banking portal meets the general obligations for access interfaces (SCA-RTS Article 30). This includes providing a means for the AISP or PISP to be identified and ensuring the AISP or PISP can rely on the authentication procedures provided by the ASPSP to the customer.

17.168 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

17.169 SCA-RTS Article 33(3) requires ASPSPs, AISPs and PISPs 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.

17.170 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).

17.171 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.

How to report

17.172 Details of how to report can be found in Chapter 13 and SUP 15.14.

What to report

17.173 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

17.174 Where an ASPSP, AISP, PISP or CBPII believes that an ASPSP's interface is not performing in compliance with Article 32, it must submit SUP 16 Annex 13 and include a short summary of the reasons it believes 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 and PISPs 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

17.175 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 and PISPs 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.

17.176 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) and SCA-RTS Article 36(1)(a). These provisions should be read in conjunction with our guidance in section 17.30 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.

17.177 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.

17.178 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), providing a brief description.

17.179 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 might provide include:

- Unavailability after 5 consecutive requests of information on the initiation of the payment transaction and all information accessible to the account servicing payment service provider 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[37].

~~17.78~~17.180 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.

[37] See section 17.59 for more guidance on sensitive payments data

18. Operational and security risks

Introduction

18.1 All PSPs are required by 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 2017.38

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 framework and establishing and implementing preventive security measures (as set out in Guidelines 2 and 4 of the EBA Guidelines).

[38] 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

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 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").[39]

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.[40]

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 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.

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

[39] See specifically 4.54 to 4.58 of Chapter 4 – Changes in circumstances of authorisation or registration.
[40] Finalised Guidance FG 16/5 'Guidance for firms outsourcing to the 'cloud' an other third-party IT services' (July 2016). Available at https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf

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[41] 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.[42]

18.16 PSPs that choose not to apply strong customer authentication under Article 17 of Commission Delegated Regulation (EU) 2018/389[43] (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. **Chapter 20 – Authentication** (section 20.55 - 20.60) provides further information.

Best practice standards

~~18.16~~18.17 PSPs should review our joint statement with HM Treasury on third party access provisions in PSD2.[44] 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.[45]

[41] 56 https://www.handbook.fca.org.uk/handbook/SYSC/
[42] See from 17.51 to 17.59
[43] The SCA-RTS is available here https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN
[44] 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
[45] 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).

20. Authentication

[…NEW CHAPTER FOR CONSULTATION…]

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 read 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[46] (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[47] 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[48]
- requirements for common and secure open standards of communication.

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. We would encourage PSPs to consider adopting a real-time risk analysis approach on a

[46] 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

[47] 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

[48] 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.

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. 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 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).

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 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, 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. 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[49] 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[50]).

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 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 information is printed on a payment card, such as the card verification number (CVV) and expiry date, it cannot be used as a knowledge factor. It may however be used as evidence of the possession of a card, alongside use of an entirely separate factor. 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.

[49] Strong customer authentication is defined in regulation 2 of the PSRs 2017

[50] 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.

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). Use of a card reader can also validate that a payment card is in the possession of the legitimate payment service user.

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 expect firms to consider the impact of strong customer authentication solutions on different groups of customers. As part of the design process, PSPs should take into account customers' different circumstances. For example, not all payment service users will possess a mobile phone or smart phone.

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 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 17.130 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 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 do 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 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.

20.30 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).

20.31 In addition, SCA-RTS Article 4(3)(d) means that a payment service user, after successfully authenticating to access their payment account, should be 'logged off' online banking after no more than 5 minutes of inactivity has elapsed.

Dynamic linking

20.32 Regulation 100(2) of the PSRs 2017 and SCA-RTS Article 5, requires 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 a payee agreed to by the payer when initiating the transaction. Accordingly, any change to the amount or the payee must invalidate the authentication code generated.

20.33 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.

20.34 In relation to card-based transactions where the amount is not known in advance (see section 8.225 – 8.229), 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. In line with SCA-RTS Recital 5, this equates to the maximum amount to which the payer has given consent. In the event that the actual amount is higher than the pre-authorised amount, even if only incrementally, the payer's PSP (the card issuer) must re-apply strong customer authentication, unless an exemption is used.

20.35 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, 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.

Exemptions from strong customer authentication

20.36 Regulation 100(5) refers of the PSRs 2017 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 of the payment transaction in accordance with Article 98(3) of PSD2. This section sets out our views on each exemption.

20.37 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)

20.38 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.

20.39 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 card 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.

20.40 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.

Payment account information (SCA-RTS Article 10)

20.41 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.

20.42 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.

20.43 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.

20.44 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.

20.45 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 separate process for this purpose.

We encourage firms and API initiatives to look for ways to facilitate and to streamline this process.

Contactless payments at point of sale and low-value transactions (SCA-RTS Articles 11 and 16)

20.46 In the context of contactless payments at point of sale (SCA-RTS Articles 11) and low-value transactions (SCA-RTS Articles 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.

20.47 The EBA Opinion (paragraph 42) states that 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)

20.48 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)

20.49 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.

20.50 Strong customer authentication is required when a payer creates or amends a list of trusted beneficiaries.

Recurring transactions (SCA-RTS Article 14)

20.51 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.

20.52 In our view, where a payer sets up electronically a card-based continuous payment authority (sometimes referred to as a merchant-initiated transaction), strong customer authentication will be required. Subsequent payments, while being out of scope of the application of strong customer authentication because they are initiated by the payee (eg

the merchant), remain subject to the transaction monitoring requirements set out in SCA-RTS Article 2.

20.53 Direct debits are out of scope of the SCA-RTS, as they are payee-initiated, unless the payer's consent for a direct debit transaction is given in the form of an electronic mandate with the involvement of its PSP. 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)

20.54 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)

20.55 Under SCA-RTS Article 17 PSPs are allowed to not 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 PSD2. There is no requirement for firms to inform us in advance that they intend to operate under this exemption but 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.

20.56 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 incorporated entity, which would include companies and limited liability partnerships.

20.57 It is also our view that the term 'dedicated payment processes or protocols' refers to payment processes and the exchange or transmission of data between devices carried out within closed networks or access-controlled environments. Examples include the use of proprietary automated host-to-host (machine-to-machine) restricted networks[51], and lodged or virtual cards, such as those used within the corporate travel management industry.

20.58 In our view, the use of standard online business banking solutions or physical corporate cards issued to employees for business expenditure would not fall within the scope of this exemption.

20.59 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

[51] Such networks often employ Public Key Infrastructure-based ('PKI') security systems and involve a dynamic connection between a company and its banking partners to enable the automated transfer of data to execute payments.

and a statement by the PSP that those levels of security are equivalent to those provided for by PSD2.

20.60 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 fraud prevention, security and encryption measures[52], which enable the secure transmission of data, 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, is below that recorded for equivalent payment transactions made via channels where strong customer authentication is applied.

Transaction risk analysis and calculation of fraud rates (SCA-RTS Articles 18 and 19)

20.61 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).

20.62 One of the conditions 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 20.67 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.

20.63 The EBA Opinion clarifies that the calculation of the fraud rate should be based on fraud data defined in the EBA Guidelines on fraud reporting[53]. 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').

20.64 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

[52] 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.

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.

20.65 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)

20.66 PSPs that use the transaction risk analysis exemption are required to immediately report to us 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. 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)

20.67 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.

20.68 As specified in SCA-RTS Article 21(2), PSPs should be prepared to provide us with the results of the monitoring, upon our request.

20.69 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. This includes the data on unauthorised transactions and fraudulent transactions resulting from the manipulation of the payer[54] 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**.

[54] '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 4
Compatibility statement

Compliance with legal requirements

1. When consulting on new rules, we are required by section 138I(2) of the Financial Services and Markets Act (FSMA) to include:

   - an explanation of how our proposals are compatible with our strategic objective and advance one or more of our operational objectives
   - an explanation of how we have had regard to the regulatory principles set out in section 3B of FSMA
   - a statement on whether the proposed rules will have a significantly different impact on mutual societies as opposed to other authorised persons

2. The requirements of section 138I do not apply to our proposals for guidance or directions under the PSRs 2017. However, under the PSRs 2017, when determining the general policy and principles by reference to which we perform particular functions under those regulations we will be required to have regard to the principles set out in regulation 106 (3) of the PSRs 2017. These mirror the principles in Section 3B FSMA.

3. This Annex also includes our assessment of the equality and diversity implications of these proposals.

4. Under the Legislative and Regulatory Reform Act 2006 (LRRA) the FCA is subject to requirements to have regard to a number of high-level 'Principles' in the exercise of some of our regulatory functions and to have regard to a 'Regulators' Code' when determining general policies and principles and giving general guidance (but not when exercising other legislative functions like making rules). This Annex sets out how we have complied with requirements under the LRRA.

The FCA's objectives and regulatory principles: Compatibility statement

5. Our proposed Handbook changes and guidance are compatible with our strategic objective of ensuring that the relevant markets function well.

6. Most of our changes primarily give effect to policies put in place by PSD2 and the PSRs 2017, and so contribute to fulfilling their aims. These correspond closely with our operational objectives of ensuring an appropriate level of consumer protection and promoting effective competition in the interests of consumers.

7. Our proposals to request specific data about Authorised Push Payment (APP) fraud complaints from PSPs and Credit Unions, will help advance our objective of ensuring an

appropriate level of consumer protection by requiring PSPs and Credit Unions to report to us on how they are meeting their obligations to consumers, and better enabling us to take supervisory action as a result of detriment identified.

Compatibility with the principles of good regulation and regulation 106 of the PSRs 2017

8. In preparing the proposals set out in this consultation paper, we have had regard to the regulatory principles set out in section 3B of FSMA and regulation 106 of the PSRs 2017. We set out below how our proposals are compatible with each principle.

The desirability of exercising our functions in a way that recognises differences in the nature and objectives of businesses carried on by different persons

9. We do not believe that our proposals discriminate against any particular business model or approach. We have considered specific requirements for PSPs conducting new payment services, account information service (AIS), payment initiation service (PIS) and card based payment instrument issuers (CBPIIs).

10. We have provided detailed guidance in our revised Approach Document, to recognise the different needs of smaller PSPs, including those new to regulation.

The principle that we should exercise our functions as transparently as possible

11. We believe that by consulting on our proposals we are acting in accordance with this principle. We are also choosing to set out detailed guidance in our Approach Document to help PSPs navigate through the PSRs 2017, various European Banking Authority (EBA) guidelines and regulatory technical standards and our relevant rules and guidance, and to understand our approach.

The need to use our resources in the most efficient and economic way

12. For the proposals in this CP, in the limited areas where we have discretion in implementing PSD2, we have had regard to the burden on the FCA in assessing how best to implement.

13. We have designed the notifications required when a PSP's fraud rate is exceeded and when there are problems with the dedicated interface to be efficient for us to process, as well as for firms to complete.

The principle that a burden or restriction should be proportionate to the benefits

14. We believe the proposals in this CP containing burdens or restrictions are proportionate to the benefits, and set out our analysis of the costs and benefits of our proposals in our CBA.

The desirability of publishing information relating to persons subject to requirements imposed under FSMA, or requiring persons to publish information

15. We have the power to publish information relating to investigations into businesses authorised under FSMA, the PSRs 2017 and the EMRs, and individuals. We are proposing to publish some of the data relating to complaints about APP fraud on the FCA website. These data will be visible to PSPs and consumers and assist with transparency on the issue of APP fraud.

The desirability of sustainable growth in the economy of the United Kingdom in the medium or long term

16. The proposals support implementation of PSD2, which seeks to improve competition in payment services, and improve access for payment services businesses.

17. We propose further guidance on the access that must be provided by ASPSPs to AISPs or PISPs. These newly regulated services could allow customers to share information about their payment accounts to improve their ability to manage their money, and increase the payment options for customers paying online products and services.

18. Our proposals have the potential to accelerate payment services innovation. This could lead to greater choice for customers, who could benefit from more flexibility about how they access their accounts and make payments. Competition pressures could also mean that customers pay lower prices for the payment services they access. This innovation and competition could contribute to growth in the payment services sector and in turn the UK's economy.

The general principle that consumers should take responsibility for their decisions

19. We do not propose any requirements which are inconsistent with this principle.

The responsibilities of senior management

20. We believe the proposals in this CP are consistent with this principle. Senior managers of PSPs will need to ensure compliance with the PSRs 2017, SCA-RTS and PSD2 and the relevant parts of our Handbook.

Expected effect on mutual societies

21. Section 138K of FSMA requires us to provide an opinion on whether the impact of a proposed rule on mutual societies is significantly different to the impact on other authorised persons.

22. We are proposing changes to The Credit Unions Sourcebook (CREDS), in order to require credit unions to report data on complaints about APP fraud. These amendments will apply to credit unions, which are mutual societies.

23. Our proposals are intended to increase consumer protection to make sure businesses have secure systems in place to minimise the risk of fraud where online transactions are offered.

24. Our proposals take into consideration credit unions' business models. We do not propose to extend all of the complaints reporting which payment service providers (subject to the PSRs 2017) must provide. This is so we do not impose a disproportionate impact on Credit Unions. While we recognise that our proposals will have an impact on Credit Unions, we are satisfied that the impact is not significantly different to that on other authorised firms.

25. Our other proposals relate to the implementation of the PSRs 2017. The PSRs 2017 do not apply to Credit Unions, and we are satisfied that the impact of our proposals on other mutual societies, such as building societies, are not significantly different to that on other authorised firms.

Equality and diversity

26. We are required under the Equality Act 2010 in exercising our functions to 'have due regard' to the need to eliminate discrimination, harassment, victimisation and any other conduct prohibited by or under the Act, advance equality of opportunity between persons who share a relevant protected characteristic and those who do not, and to foster good relations between people who share a protected characteristic and those who do not.

27. As part of this, we ensure the equality and diversity implications of any new policy proposals are considered.

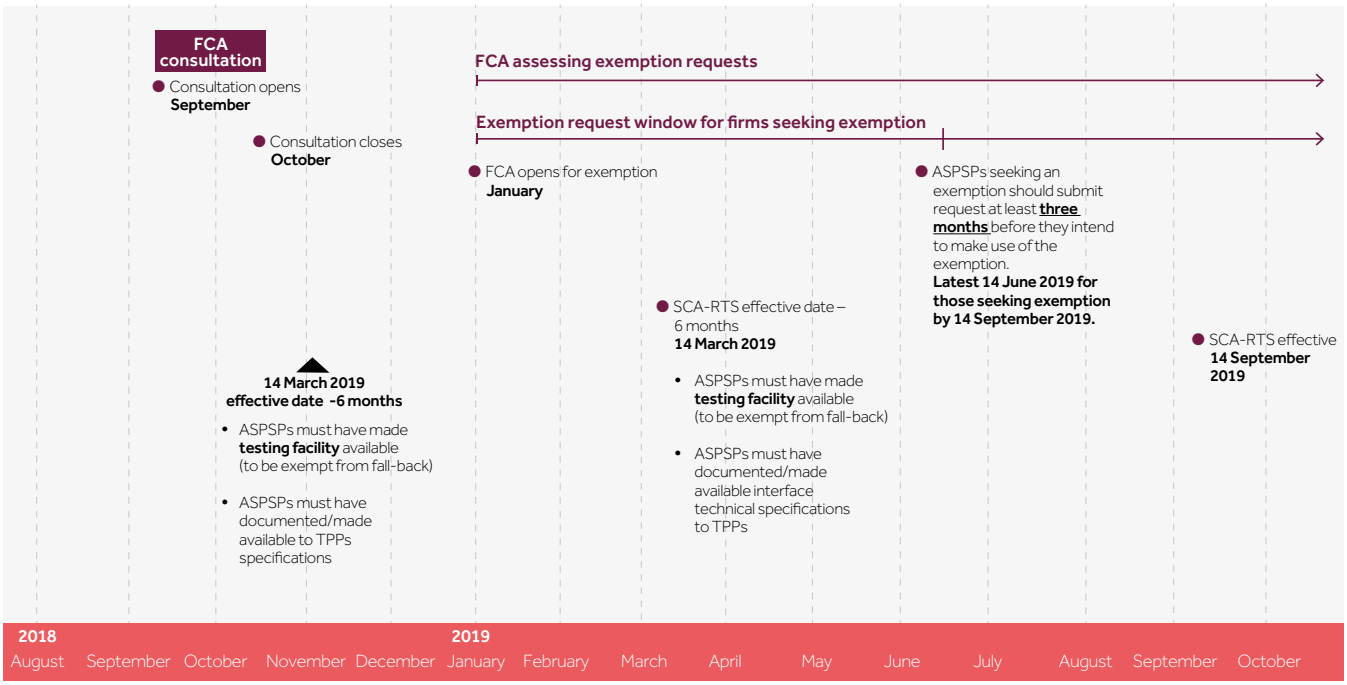
28. The outcome of our consideration in relation to these matters in this case is stated in paragraph 2.20 of the Consultation Paper.

Legislative and Regulatory Reform Act 2006 (LRRA)

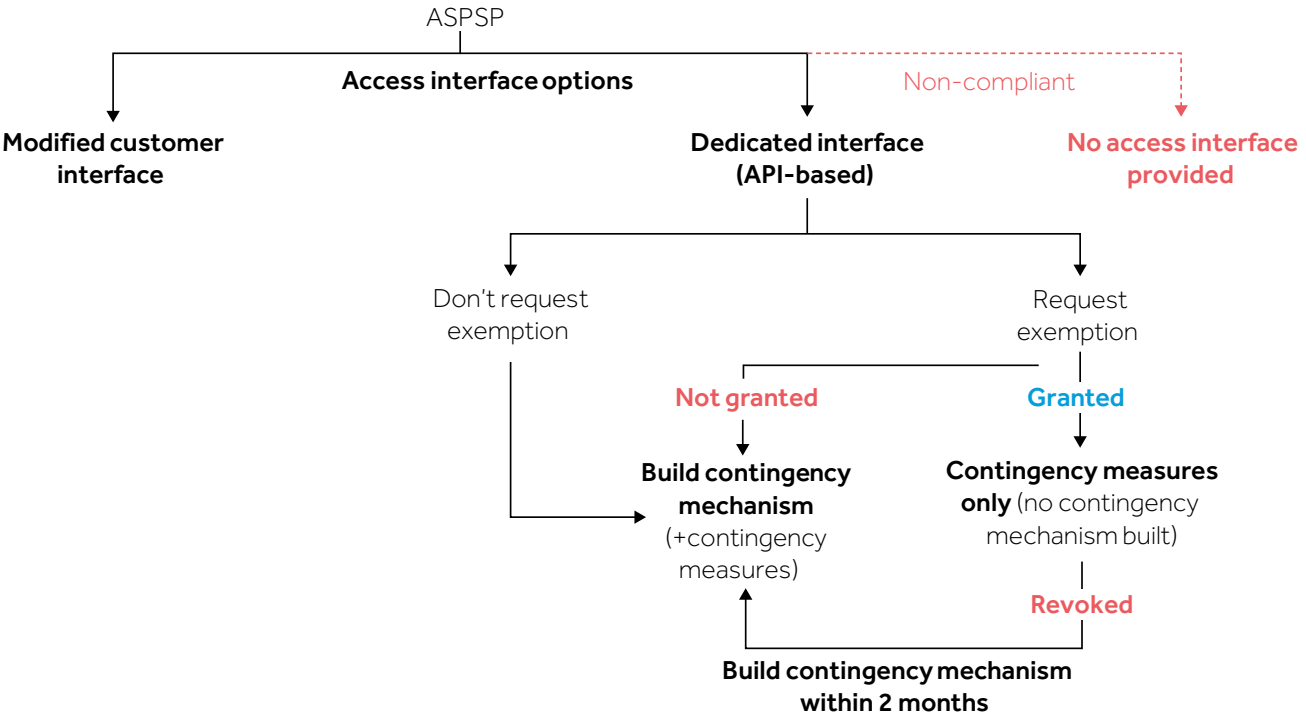
29. We have had regard to the principles in the LRRA and the Regulators' Code for the parts of the proposals that consist of general policies, principles or guidance and consider that our proposals are proportionate and result in an appropriate level of consumer protection, when balanced with impacts on businesses and on competition.

Annex 5
Timeline and process for contingency mechanism exemption request

Contingency mechansim exemption timeline



Contingency measures, contingency mechanism, exemption and revocation for dedicated interfaces



Annex 6
Abbreviations in this document

AIS	Account information service
API	Application programming interface
APP	Authorised push payment
ASPSP	Account servicing payment service provider
CBA	Cost benefit analysis
CBPII	Card-based payment instrument issuer
CP	Consultation paper
CREDS	The Credit Union sourcebook
DISP	Dispute Resolution: Complaints sourcebook
EMI	Electronic money institution
EBA	European Banking Authority
FSMA	Financial Services and Markets Act
LNE	Limited network exclusion
LRRA	Legislative and Regulatory Reform Act
OBIE	Open Banking Implementation Entity
PERG	Perimeter Guidance Manual
PI	Payment institution
PIS	Payment initiation service
PSD2	Revised Payment Services Directive
PSP	Payment service provider
PSR	Payment Systems Regulator
RAISP	Registered account information service provider

RTS	Regulatory Technical Standard
SCA-RTS	RTS on strong customer authentication and common and secure communication
TPP	Third-party provider

We have developed the policy in this Consultation Paper in the context of the existing UK and EU regulatory framework. The Government has made clear that it will continue to implement and apply EU law until the UK has left the EU. We will keep the proposals under review to assess whether any amendments may be required in the event of changes in the UK regulatory framework in the future.

We make all responses to formal consultation available for public inspection unless the respondent requests otherwise. We will not regard a standard confidentiality statement in an email message as a request for non-disclosure.

Despite this, we may be asked to disclose a confidential response under the Freedom of Information Act 2000. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by the Information Commissioner and the Information Rights Tribunal.

All our publications are available to download from www.fca.org.uk. If you would like to receive this paper in an alternative format, please call 020 7066 7948 or email: publications_graphics@fca.org.uk or write to: Editorial and Digital team, Financial Conduct Authority, 12 Endeavour Square, London E20 1JN

Appendix 1
Draft Handbook text

PAYMENT SERVICES INSTRUMENT 2018

Powers exercised by the Financial Conduct Authority

A. The Financial Conduct Authority makes this instrument in the exercise of the powers and related provisions in or under:

(1) the following sections of the Financial Services and Markets Act 2000 ("the Act"):

(a) section 137A (The FCA's general rules) (including as applied by paragraph 3 of part 1 of Schedule 6 of the Payment Services Regulations 2017);
(b) section 137T (General supplementary powers) (including as applied by paragraph 3 of part 1 of Schedule 6 of the Payment Services Regulations 2017);
(c) section 139A (Power of the FCA to give guidance);
(d) paragraph 13(4) of Schedule 17 (FCA's rules);

(2) the following regulations of the Regulations:

(a) regulation 30(4) and (5) (Supervision of firms exercising passport rights);
(b) regulation 98(3) (Management of operational and security risks);
(c) regulation 109 (Reporting requirements); and
(d) regulation 120 (Guidance).

B. The rule-making powers listed above are specified for the purpose of section 138G(2) (Rule-making instruments) of the Act.

Commencement

C. This instrument comes into force on 19 December 2018 except for part 2 of Annex B which comes into force on 1 January 2019 and part 3 of Annex B and part 2 of Annex F which come into force on 14 September 2019.

Amendments to the Handbook

D. The modules of the FCA's Handbook of rules and guidance listed in column (1) below are amended in accordance with the Annexes to this instrument listed in column (2) below:

(1)	(2)
Glossary of definitions	Annex A
Supervision manual (SUP)	Annex B
Dispute Resolution: Complaints sourcebook (DISP)	Annex C
Credit Unions sourcebook (CREDS)	Annex D
Banking Conduct of Business sourcebook (BCOBS)	Annex E

Amendments to material outside the Handbook

E. The Perimeter Guidance manual (PERG) is amended in accordance with Annex F to this instrument.

Notes

F. In this instrument, the "notes" (indicated by "**Note:**") are included for the convenience of readers but do not form part of the legislative text.

Citation

G. This instrument may be cited as the Payment Services Instrument 2018.

By order of the Board
[*date*]

Annex A

Amendments to the Glossary of definitions

In this Annex, underlining indicates new text and striking through indicates deleted text unless otherwise stated.

The following definition was published in CP18/16 and is included here for reference only.

authorised push payment fraud	a transfer of funds by a *payer* to a *person* where: (1) the *payer* intended to transfer the funds to a certain *person* but was instead deceived into transferring the funds to a different *person*; or (2) the *payer* transferred funds to another *person* for what they believed were legitimate purposes but which were in fact fraudulent.

Insert the following new definitions in the appropriate alphabetical position. The text is not underlined.

SCA RTS	Regulation (EU) 2018/389 (RTS) on strong customer authentication and common and secure communication.

Amend the following definitions as shown

electronic money	electronically (including magnetically) stored monetary value as represented by a claim on the *electronic money issuer* which is: (a) issued on receipt of funds for the purpose of making payment transactions as defined in Article 4(5) of the *Payment Services Directive*; and (b) accepted by a *person* other than the *electronic money issuer*; but does not include: (c) monetary value stored on specific *payment instruments* that can ~~be used to acquire goods or services only~~ only be used in a limited way and meet one of the following conditions: (i) ~~in or on the *electronic money issuer's* premises; or~~ allow the holder to acquire goods or services only in the issuer's premises; (ii) ~~under a commercial agreement with the *electronic money issuer*, either within a limited network of service~~

~~providers or for a limited range of goods or services; or~~ are issued by a professional issuer and allow the holder to acquire goods or services only within a limited network of service providers which have a direct commercial agreement with the issuer;

(iii) may be used only to acquire a very limited range of goods or services; or

(iv) are valid only in a single *EEA State*, are provided at the request of an undertaking or a public sector entity, and are regulated by a national or regional public authority for specific social or tax purposes to acquire specific goods or services from suppliers which have a commercial agreement with the issuer.

(d) ~~monetary value that is used to make payment transactions executed by means of any telecommunication, digital or IT device, where the goods or services purchased are delivered to and are to be used through a telecommunication, digital or IT device, provided that the telecommunication, digital or IT operator does not act only as an intermediary between the payment service user and the supplier of the goods and services.~~

monetary value that is used to make *payment transactions* resulting from services provided by a provider of electronic communications networks or services, including transactions between persons other than that provider and a subscriber, where those services are provided in addition to electronic communications services for a subscriber to the network or service, and where the additional service is:

(i) for purchase of *digital content* and voice-based services, regardless of the device used for the purchase or consumption of the digital content, and charged to the related bill; or

(ii) performed from or via an electronic device and charged to the related bill for the purchase of tickets or for donations to organisations which are registered or recognised as charities by public authorities, whether in the *United Kingdom* or elsewhere,

provided that the value of any single *payment transaction* does not exceed £40, and the cumulative value of *payment transactions* for an individual subscriber in a month does not exceed £240.

Annex B

Amendments to the Supervision manual (SUP)

In this Annex, underlining indicates new text and striking through indicates deleted text unless otherwise stated.

Part 1. Comes into force on 18 December 2018.

Insert the following new section after SUP 15B (Applications and notifications under the benchmarks regulation and powers over Miscellaneous BM persons). The text is not underlined.

15C	**Applications under the Payment Services Regulations**	
15C.1	**Application**	
15C.1.1	R	This chapter applies to *payment service providers*.
15C.2	**Request for exemption from the obligation to set up a contingency mechanism (Article 33(6) of the SCA RTS)**	
15C.2.1	G	*Account servicing payment service providers* that opt to provide a dedicated interface under Article 31 of the *SCA RTS* may request that the *FCA* grant an exemption from the obligation in Article 33(4) to set up a contingency mechanism. The exemption will be granted if the dedicated interface meets the conditions set out in Article 33(6).
15C.2.1	D	*Account servicing payment service providers* wishing to rely on the exemption in Article 33(6) of the *SCA RTS* must submit to the *FCA* the form specified in *SUP* 15C Annex 1 by electronic means made available by the *FCA.*
15C.2.2	G	*Account servicing payment service providers* are encouraged to discuss an exemption request with their usual supervisory contact as early as possible, and before submitting the form in *SUP* 15C Annex 1.
15C.2.3	G	The *EBA* issued Guidelines on [insert date final guidelines issued] on the conditions to be met to benefit from an exemption from contingency measures under Article 33(6) of the *SCA RTS*. The Guidelines clarify the requirements *account servicing payment service providers* need to meet to obtain an exemption and the information competent authorities should consider to ensure the consistent application of these requirements across jurisdictions. The *FCA* provides further guidance on making an exemption request in paragraphs 17.98 to 17.166 of the *FCA's* Approach Document.

		Note: see [insert link to final EBA guidelines] and https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf.
15C.2.4	D	When completing the form specified in *SUP* 15C Annex 1, *account servicing payment service providers* must provide to the *FCA* such information as is necessary to enable the *FCA* to determine whether the requirements in Guidelines 2 to 8 of the *EBA's* Guidelines on the conditions to be met to benefit from an exemption from contingency measures under Article 33(6) of the *SCA RTS* are met.
15C.2.5	G	*Account servicing payment service providers* should note that Article 16(3) of Regulation (EU) No. 1093/2010 also requires them to make every effort to comply with the *EBA*'s Guidelines on the conditions to be met to benefit from an exemption from contingency measures under Article 33(6) of the *SCA RTS*.

15C Annex 1	**D**	**Form: Request for exemption from the obligation to set up a contingency mechanism (Article 33(6) of the SCA RTS)**

Request for exemption from the obligation to set up a contingency mechanism (Article 33(6) of the *SCA RTS*)

Where a group of ASPSPs or a single ASPSP operates a number of dedicated interfaces, e.g. in respect of different banking brands, we require separate requests in respect of each dedicated interface for which an ASPSP is seeking an exemption.

D1	Financial Registration Number (FRN):	
D2	Identifying feature of the dedicated interface for which the exemption is sought, e.g. name of brand or entity	
D4	Contact person name	
D5	Contact role within organisation	
D6	Contact DDI phone number	
D7	Contact email address	

Please record the filenames for any attachments provided to support this request.

Q10	<Enter filename>	<Enter filename>	<Enter filename>
Q13	<Enter filename>	<Enter filename>	<Enter filename>
Q16	<Enter filename>	<Enter filename>	<Enter filename>
Q17	<Enter filename>	<Enter filename>	<Enter filename>
Q25	<Enter filename>	<Enter filename>	<Enter filename>

Guidance on completing the form can be found in the Payment Services and Electronic Money Approach Document, Chapter 17.

Note: see https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf.

ASPSPs completing the form should also comply with the [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) (EBA Guidelines).

Note: see [Link to be inserted when final].

	Service level, availability and performance (EBA Guideline 2)	
Q1	Confirm that the ASPSP has the same service level objectives and targets, out of hours support, monitoring and contingency plans as it has in place for the interface(s) used by its own payment service users, as per EBA Guideline 2.1.	Yes/No
Q2	Confirm that the ASPSP has in place the key performance indicators of availability described in EBA Guideline 2.2 for both its dedicated interface and each of the interfaces used by its payment service users (PSUs).	Yes/No
Q3	Confirm that the ASPSP has in place the key indicators of performance described in EBA Guideline 2.3 for its dedicated interface.	Yes/No
Q4	Confirm that the key performance indicators are calculated in accordance with EBA Guideline 2.4.	Yes/No
	Publication of indicators (EBA Guideline 3)	
Q5	Plan for publication: Should include: • the planned date of the first publication • a brief description, including website address if possible, of where the statistics will be published on the ASPSP's website.	dd/mm/yyyy Up to 500 words
Q6	Confirm that the publication each quarter will present daily statistics on a quarterly basis on availability and performance as set out in Guideline 2.2 and 2.3 of the EBA Guidelines for the dedicated	Yes/No

	interface and each payment service user interface together.	
Q7	Confirm that, from the date of first publication, the publication will provide a comparison of the availability of the ASPSP's dedicated interface with its best-performing PSU interface.	Yes/No
	Stress testing (EBA Guideline 4)	
Q8	Confirm that adequate stress testing has been undertaken in accordance with EBA Guideline 4.2 a-d.	Yes/No
Q9	A summary of the result of the stress testing covering points a-d, including any weaknesses or issues identified and confirmation that these have been addressed. As part of this, you should inform us whether the views of AISPs, PISPs and CBPIIs, or representatives of these market participants were sought about likely peak usage periods or other stresses.	Up to 2,000 words
	Obstacles (EBA Guideline 5)	
Q10	Summary of the methods of access chosen by the ASPSP	Optional file attachment of illustrations
	Redirection	Summary - up to 500 words
	Decoupled	Summary- up to 500 words
	Embedded	Summary - up to 500 words
	Other	Summary - up to 500 words
Q11	Where the ASPSP has put in place only one method of access, please explain the reasons why this method of access is not an obstacle as referred to in Article 32(3) of the SCA-RTS and how this method of access supports all authentication methods provided by the ASPSP to its PSU.	Up to 2,000 words
Q12	Confirm that the interface meets the requirements of EBA Guideline 5.2 a – d.	Yes/No
Q13	Provide a visual representation of the customer journey when a payment service user accesses their payment account via PISP or AISP (including any authentication steps that take place in the ASPSP's domain).	File attachment(s)
	Design and testing to the satisfaction of PSPs (EBA Guideline 6)	
Q14	Confirm that the ASPSP has published a summary of the technical specification of the dedicated interface on its website. An ASPSP will need to provide a web link	Yes/No URL:

	(URL) to the webpage where the technical specifications are provided.	
Q15	Confirm that the ASPSP has made available a testing facility for the dedicated interface that allows AISPs, PISPs and CBPIIs to test the dedicated interface in relation to points a-f in EBA Guideline 6.2 and the date from which the testing facility was made available.	Yes/No Date from which the testing facility was available
Q16	Provide 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.	Up to 2,000 words
Q17	Provide details of which initiative standard is being implemented (as per EBA Guideline 6.4(a)).	e.g. Open Banking, Berlin Group etc
Q18	Provide the results of conformance testing of the implemented API against an initiative standard, for example, completed conformance checklist.	File attachment
Q19	Provide details of whether, and if so how and why, the ASPSP has deviated from any standard implementation requirements of the initiative, if available, as per EBA Guideline 6.4(b).	Up to 2,000 words
Q20	Where an ASPSP is not implementing a market initiative standard, a description as to the form of engagement that has taken place with PISPs, AISPs and CBPIIs for implementing the dedicated interface as per EBA Guideline 6.5.	Up to 2,000 words
Q21	Where an ASPSP is not implementing a market initiative standard, a completed PSD2 checklist based on the EBA Opinion 'Table 1 – Main requirements for dedicated interfaces and API initiatives'.	Up to 2,000 words
	Wide usage of the interface (EBA Guideline 7)	
Q22	Provide the number of PISPs, CBPIIs, AISPs and PSPs (including those not yet authorised that have applied for the relevant authorisation) that have made use of the testing facility.	Number
Q23	Provide the number of AISPs, PISPs and CBPIIs that are using the interface. In our view, use of the interface means that ASPSPs will have enabled AISPs, PISPs and CBPIIs to use their API interface to provide their services in a live environment to their customers for 3 months.	Number

Q24	Describe which aspects of the interface have been used by AISPs, PISPs, or CBPIIs	e.g. AISP functionality, PISP functionality, CBPII functionality, none, all
Q25	Describe the measures undertaken to ensure that the availability of the testing facilities for these aspects has been well publicised via appropriate channels, including where appropriate the website of the ASPSP, social media, industry trade bodies, conferences and direct engagement with known market actors. We expect the ASPSP to demonstrate that at least 3 months of communication of the testing facilities has taken place.	Yes/No
	Resolution of problems (EBA Guideline 8)	
Q26	Describe the systems or procedures in place for tracking, resolving and closing problems, including those reported by PISPs, AISPs and CBPIIs. This should include describing out of hours support, service level objectives for problems resolution, ticketing systems for issues raised.	Up to 2,000 words
Q27	Confirm that the service level for dedicated interface problem resolution is equivalent to the service level for resolving problems with the interface used by the ASPSP's own payment service users (as per EBA Guideline 2.1). This should include an outline of what the service level targets are for each.	Up to 2,000 words
Q28	As per EBA Guideline 8.1(b), an explanation of the problems that have not been resolved without undue delay in accordance with the service level targets and support detailed in EBA Guideline 2.1.	Up to 2,000 words

Checklist for ASPSPs not implementing a market initiative

Requirement	**Article**	**Does the dedicated interface meet the regulatory requirements?**
Enabling CBPIIs, AISPs and PISPs to access the necessary data from payment accounts accessible online	Article 65, 66 & 67 PSD2 Article 30 RTS	Yes/No
Conforming to (widely used) standard(s) of communication issued by international or European standardisation organisations	Article 30(3) RTS	Yes/No
Allowing the PSU to authorise and consent to a payment transaction via a PISP	Article 64(2) of PSD2 Article 30(1)(c) RTS	Yes/No
Enabling PISPs and AISPs to ensure that when they transmit the personalised security credentials issued by the ASPSP, they do so through safe and efficient channels.	Article 66(3)(b) and 67(2)(b) PSD2	Yes/No
Enabling the identification of the AISP/PISP/CBPII and support eIDAS certificates	Article 65(2)(c), 66(2)(d) and 67(2)(c) PSD2 Article 30(1) (a) and 34 RTS	Yes/No
Allowing for 90 days re-authentication for AISPs	Article 10(2)(b) RTS	Yes/No
Enabling the ASPSPs and AISPs to count the number of access requests during a given period	Article 36(5) RTS	Yes/No
Allowing for a change control process	Article 30(4) RTS	Yes/No
Allowing for the possibility for an initiated transaction to be cancelled in accordance with PSD2, including recurring transactions	Article 64(2) and 80(2) PSD2 and 80(4)	Yes/No
Allowing for error messages explaining the reason for the unexpected event or error	Articles 36(2) RTS	Yes/No
Supporting access via technology service providers on behalf of authorised actors	Article 19(6) PSD2	Yes/No
Allowing AISPs and PISPs to rely on all authentication	Article 97(5) PSD2 Article 30(2) RTS	Yes/No

Requirement	Article	Does the dedicated interface meet the regulatory requirements?
procedures issued by the ASPSP to its customers		
Enabling the AISP to access the same information as accessible to the individual consumer and corporates in relation to their designated payment accounts and associated payment transactions	Art 67(2)(d) PSD2 Articles 30(1)(b) and 36(1)(a) RTS	Yes/No
Enabling the ASPSP to send, upon request, an immediate confirmation yes/no to the PSP (PISP and CBPII) on whether there are funds available	Article 36(1)(c) RTS	Yes/No
Enabling the dynamic linking to a specific amount and payee, including batch payments	Article 97(2) PSD2 Article 5 RTS	Yes/No
Enabling the ASPSP to apply the same exemptions from SCA for transactions initiated by PISPs as when the PSU interacts directly with the ASPSP	Articles 30(2), 32(3), 18(2)(c)(v) and (vi) and 18(3) RTS	Yes/No
Enabling strong customer authentication composed of two different elements	Article 4 RTS	Yes/No
Enabling a secure data exchange between the ASPSP and the PISP, AISP and CBPII mitigating the risk for any misdirection of communication to other parties	Articles 28 & 35 RTS	Yes/No
Ensuring security at transport and application level	Article 97(3) PSD2 Articles 30(2)(c) and 35 RTS	Yes/No
Supporting the needs to mitigate the risk for fraud, have reliable and auditable exchanges and enable providers to monitor payment transactions	Article 97(3) PSD2 Articles 22, 35 and 3 RTS	Yes/No
Allowing for traceability	Article 29 RTS	Yes/No
Allowing for the ASPSP's dedicated interface to provide at least the same availability	Article 32 RTS	Yes/No

Requirement	Article	Does the dedicated interface meet the regulatory requirements?
and performance as the user interface		

Part 2. Comes into force on 1 January 2019.

Amend the following text as shown.

16	**Reporting requirements**	
…		
16.13	**Reporting under the Payment Services Regulations**	
…		
	Reporting requirement	
…		
	Statistical data on fraud	
…		
16.13.7	D	This statistical data on fraud must be submitted to the *FCA* by electronic means made available by the *FCA* using the format of the return set out in *SUP* 16 Annex 27ED. Guidance notes for the completion of the return are set out in *SUP* 16 Annex 27FG.
16.13.8	G	The return set out in *SUP* 16 Annex 27ED must be provided to the *FCA* ~~at least once~~ every six months ~~per year~~ (this does not apply to *small payment institutions, registered account information service providers and small electronic money institutions*). The first return should cover the period beginning on 1 January 2019 and ending on 30 June 2019 ~~13 January 2018 and ending on 31 December 2018~~ and should be submitted by 31 ~~January~~ July 2019. Subsequent returns should cover consecutive reporting periods of ~~one year~~ 6 months ~~beginning on 1 January and ending on 31 December each year~~ and should be submitted within 2 *months* ~~1 *month*~~ of the end of the reporting period. *Small payment institutions, registered account information service providers and small electronic money institutions* must report once per year. The first return should cover the period beginning on 1 January 2019 and ending on 31 December 2019 and should be submitted by 31 January 2020. Subsequent returns should cover consecutive reporting periods of one year and should be submitted within 2 *months* of the end of the reporting period

16.13.8A	G	*Payment service providers* should use the return in *SUP* 16 Annex 27ED to comply with the *EBA*'s Guidelines on fraud reporting. *Payment service providers* should note that Article 16(3) of Regulation (EU) No. 1093/2010 requires them to make every effort to comply with the *EBA*'s Guidelines. The return also includes fraud reporting for *registered account information service providers*, as required by regulation 109 of the *Payment Services Regulations.*
		Note: see [insert link to final EBA guidelines].

SUP 16 Annex 27E is deleted in its entirety and replaced. The new text is not underlined.

REP017 Payments Fraud Report

Table 1 - Payment transactions and fraudulent payment transactions for payment services (EBA GL)

Transactions per type of payment service

Credit transfers

		A	B	C	D	E	F	G	H	I	J	K	L
		Geo breakdown for sent transactions						Geo breakdown for sent fraudulent transactions					
		Domestic		Cross-border within EEA		Cross-border outside EEA		Domestic		Cross-border within EEA		Cross-border outside EEA	
		By volume	By value	By volume	By value	By volume	By value	By volume	By value	By volume	By value	By volume	By value
1	Total credit transfers sent												
	of which broken down by payment initiation channel												
2	Initiated non-electronically												
3	Initiated electronically												
	of which broken down by sub-channel:												
4	**Remote**												
	of which broken down by authentication method:												
5	Authenticated via Strong Customer Authentication												
	of which fraudulent credit transfers by fraud types:												
6	Issuance of a payment order by the fraudster												
7	Modification of a payment order by the fraudster												
8	Manipulation of the payer by the fraudster to issue a payment order												
9	Authenticated via non-Strong Customer Authentication												
	of which fraudulent credit transfers by fraud types:												
10	Issuance of a payment order by the fraudster												
11	Modification of a payment order by the fraudster												
12	Manipulation of the payer by the fraudster to issue a payment order												
	of which broken down by reason for authentication via non-SCA												
13	Low value (art.16 RTS)												
14	Payment to self (art.15 RTS)												
15	Trusted beneficiary (art.13 RTS)												
16	Recurring transaction (art.14 RTS)												
17	Use of secure corporate payment processes or protocols (art. 17 RTS)												
18	TRA (art.18 RTS)												
19	**Non-remote**												
	of which broken down by authentication method:												
20	Authenticated via Strong Customer Authentication												
	of which fraudulent credit transfers by fraud types:												
21	Issuance of a payment order by the fraudster												
22	Modification of a payment order by the fraudster												
23	Manipulation of the payer by the fraudster to issue a payment order												
24	Authenticated via non-Strong Customer Authentication												
	of which fraudulent credit transfers by fraud types:												
25	Issuance of a payment order by the fraudster												
26	Modification of a payment order by the fraudster												
27	Manipulation of the payer by the fraudster to issue a payment order												
	of which broken down by reason for authentication via non-SCA												
28	Payment to self (art.15 RTS)												
29	Trusted beneficiary (art.13 RTS)												
30	Recurring transaction (art.14 RTS)												
31	Contactless low value (art. 11 RTS)												
32	Unattended terminal for transport or parking fares (art. 12 RTS)												
	of which:												
33	Initiated by PISP												
	Losses borne due to fraud per liability bearer:												
34	The reporting PSP												
35	The Payment Service User (payer)												
36	Others												

Direct debits

		A	B	C	D	E	F	G	H	I	J	K	L
		Geo breakdown for sent transactions						Geo breakdown for sent fraudulent transactions					
		Domestic		Cross-border within EEA		Cross-border outside EEA		Domestic		Cross-border within EEA		Cross-border outside EEA	
		By volume	By value	By volume	By value	By volume	By value	By volume	By value	By volume	By value	By volume	By value
37	Total direct debits sent												
	of which broken down by the channel used to give consent:												
38	**Consent given via an electronic mandate**												
	of which fraudulent direct debits by fraud type:												
39	Unauthorised payment transactions												
40	Manipulation of the payer by the fraudster to consent to a direct debit												
41	**Consent given in another form than an electronic mandate**												
	of which fraudulent direct debits by fraud type:												
42	Unauthorised payment transactions												
43	Manipulation of the payer by the fraudster to consent to a direct debit												
	Losses borne due to fraud per liability bearer:												
44	The reporting PSP												
45	The Payment Service User (payer)												
46	Others												

Card payments with cards issued by resident PSP (except cards with an e-money function only)

		A	B	C	D	E	F	G	H	I	J	K	L
		Geo breakdown for sent transactions						Geo breakdown for sent fraudulent transactions					
		Domestic		Cross-border within EEA		Cross-border outside EEA		Domestic		Cross-border within EEA		Cross-border outside EEA	
		By volume	By value	By volume	By value	By volume	By value	By volume	By value	By volume	By value	By volume	By value
47	Total card payments with cards issued by resident PSP (except cards with an e-money function only)												
	of which broken down by payment initiation channel												
48	Initiated non-electronically												
49	Initiated electronically												
	of which broken down by sub-channel:												
50	**Remote**												
	of which broken down by card function:												
51	Payments with cards with a debit function												
52	Payments with cards with a credit or delayed debit function												
	of which broken down by authentication method:												
53	**Authenticated via Strong Customer Authentication**												
	of which fraudulent card payments by fraud types:												
54	Issuance of a payment order by a fraudster												
	of which broken down by fraud sub-types:												
55	Lost or Stolen card												
56	Card Not Received												
57	Counterfeit card												
58	Card details theft												
59	Other												
60	Modification of a payment order by the fraudster												
61	Manipulation of the payer to make a card payment												
62	**Authenticated via non-Strong Customer Authentication**												
	of which fraudulent card payments by fraud types:												
63	Issuance of a payment order by a fraudster												
	of which broken down by fraud sub-types:												
64	Lost or Stolen card												
65	Card Not Received												
66	Counterfeit card												
67	Card details theft												
68	Other												
69	Modification of a payment order by the fraudster												
70	Manipulation of the payer to make a card payment												
	of which broken down by reason for authentication via non-SCA:												
71	Low value (art.16 RTS)												
72	Trusted beneficiary (art.13 RTS)												
73	Recurring transaction (art.14 RTS)												
74	Use of secure corporate payment processes or protocols (art. 17 RTS)												
75	TRA (art.18 RTS)												
76	**Non-remote**												
	of which broken down by card function:												
77	Payments with cards with a debit function												
78	Payments with cards with a credit or delayed debit function												
	of which broken down by authentication method:												
79	Authenticated via Strong Customer Authentication												
	of which fraudulent card payments by fraud types:												
80	Issuance of a payment order by a fraudster												
	of which broken down by fraud sub-types:												
81	Lost or Stolen card												
82	Card Not Received												
83	Counterfeit card												
84	Card details theft												
85	Other												
86	Modification of a payment order by the fraudster												
87	Manipulation of the payer to make a card payment												
88	Authenticated via non-Strong Customer Authentication												
	of which fraudulent card payments by fraud types:												
89	Issuance of a payment order by a fraudster												
	of which broken down by fraud sub-types:												
90	Lost or Stolen card												
91	Card Not Received												
92	Counterfeit card												
93	Card details theft												
94	Other												
95	Modification of a payment order by the fraudster												
96	Manipulation of the payer to make a card payment												
	of which broken down by reason for authentication via non-SCA												
97	Trusted beneficiary (art.13 RTS)												
98	Recurring transaction (art.14 RTS)												
99	Contactless low value (art. 11 RTS)												
100	Unattended terminal for transport or parking fares (art. 12 RTS)												
	Losses borne due to fraud per liability bearer:												
101	The reporting PSP												
102	The Payment Service User (payer)												
103	Others												

Card payments with cards acquired by resident PSP (except cards with an e-money function only)

		A	B	C	D	E	F	G	H	I	J	K	L
		Geo breakdown for sent transactions						Geo breakdown for sent fraudulent transactions					
		Domestic		Cross-border within EEA		Cross-border outside EEA		Domestic		Cross-border within EEA		Cross-border outside EEA	
		By volume	By value	By volume	By value	By volume	By value	By volume	By value	By volume	By value	By volume	By value
104	Total card payments with cards acquired by resident PSP (except cards with an e-money function only)												
	of which broken down by payment initiation channel												
105	Initiated non-electronically												
106	Initiated electronically												
	of which broken down by sub-channel:												
107	**Remote**												
	of which broken down by card function:												
108	Payments with cards with a debit function												
109	Payments with cards with a credit or delayed debit function												
	of which broken down by authentication method:												
110	**Authenticated via Strong Customer Authentication**												
	of which fraudulent card payments by fraud types:												
111	Issuance of a payment order by a fraudster												
	of which broken down by fraud sub-types:												
112	Lost or Stolen card												
113	Card Not Received												
114	Counterfeit card												
115	Card details theft												
116	Other												
117	Modification of a payment order by the fraudster												
118	Manipulation of the payer to make a card payment												
119	**Authenticated via non-Strong Customer Authentication**												
	of which fraudulent card payments by fraud types:												
120	Issuance of a payment order by a fraudster												
	of which broken down by fraud sub-types:												
121	Lost or Stolen card												
122	Card Not Received												
123	Counterfeit card												
124	Card details theft												
125	Other												
126	Modification of a payment order by the fraudster												
127	Manipulation of the payer to make a card payment												
	of which broken down by reason for authentication via non-SCA:												
128	Low value (art.16 RTS)												
129	Recurring transaction (art.14 RTS)												
130	TRA (art.18 RTS)												
131	**Non-remote**												
	of which broken down by card function:												
132	Payments with cards with a debit function												
133	Payments with cards with a credit or delayed debit function												
	of which broken down by authentication method:												
134	**Authenticated via Strong Customer Authentication**												
	of which fraudulent card payments by fraud types:												
135	Issuance of a payment order by a fraudster												
	of which broken down by fraud sub-types:												
136	Lost or Stolen card												
137	Card Not Received												
138	Counterfeit card												
139	Card details theft												
140	Other												
141	Modification of a payment order by the fraudster												
142	Manipulation of the payer to make a card payment												
143	**Authenticated via non-Strong Customer Authentication**												
	of which fraudulent card payments by fraud types:												
144	Issuance of a payment order by a fraudster												
	of which broken down by fraud sub-types:												
145	Lost or Stolen card												
146	Card Not Received												
147	Counterfeit card												
148	Card details theft												
149	Other												
150	Modification of a payment order by the fraudster												
151	Manipulation of the payer to make a card payment												
	of which broken down by reason for authentication via non-SCA												
152	Recurring transaction (art.14 RTS)												
153	TRA (art.18 RTS)												
154	Contactless low value (art. 11 RTS)												
155	Unattended terminal for transport or parking fares (art. 12 RTS)												
	Losses borne due to fraud per liability bearer:												
156	The reporting PSP												
157	The Payment Service User (payer)												
158	Others												

E-money payment transactions with e-money issued by resident PSPs

		A	B	C	D	E	F	G	H	I	J	K	L
		Geo breakdown for sent transactions						Geo breakdown for sent fraudulent transactions					
		Domestic		Cross-border within EEA		Cross-border outside EEA		Domestic		Cross-border within EEA		Cross-border outside EEA	
		By volume	By value	By volume	By value	By volume	By value	By volume	By value	By volume	By value	By volume	By value
159	Total e-money payment transactions with e-money issued by resident PSPs												
	of which broken down by payment initiation channel												
160	**Remote**												
	of which broken down by authentication method:												
161	**Authenticated via Strong Customer Authentication**												
	of which fraudulent credit transfers by fraud types:												
162	Issuance of a payment order by the fraudster												
163	Modification of a payment order by the fraudster												
164	Manipulation of the payer by the fraudster to issue a payment order												
165	**Authenticated via non-Strong Customer Authentication**												
	of which fraudulent credit transfers by fraud types:												
166	Issuance of a payment order by the fraudster												
167	Modification of a payment order by the fraudster												
168	Manipulation of the payer by the fraudster to issue a payment order												
	of which broken down by reason for authentication via non-SCA:												
169	Low value (art.16 RTS)												
170	Trusted beneficiary (art.13 RTS)												
171	Recurring transaction (art.14 RTS)												
172	Use of secure corporate payment processes or protocols (art. 17 RTS)												
173	TRA (art.18 RTS)												
174	**Non-remote**												
	of which broken down by authentication method:												
175	Authenticated via Strong Customer Authentication												
	of which fraudulent credit transfers by fraud types:												
176	Issuance of a payment order by the fraudster												
177	Modification of a payment order by the fraudster												
178	Manipulation of the payer by the fraudster to issue a payment order												
179	Authenticated via non-Strong Customer Authentication												
	of which fraudulent credit transfers by fraud types:												
180	Issuance of a payment order by the fraudster												
181	Modification of a payment order by the fraudster												
182	Manipulation of the payer by the fraudster to issue a payment order												
	of which broken down by reason for authentication via non-SCA												
183	Trusted beneficiary (art.13 RTS)												
184	Recurring transaction (art.14 RTS)												
185	Contactless low value (art. 11 RTS)												
186	Unattended terminal for transport or parking fares (art. 12 RTS)												
	Losses borne due to fraud per liability bearer:												
197	The reporting PSP												
198	The Payment Service User (payer)												
199	Others												

Money remittances

		A	B	C	D	E	F	G	H	I	J	K	L
		Geo breakdown for sent transactions						Geo breakdown for sent fraudulent transactions					
		Domestic		Cross-border within EEA		Cross-border outside EEA		Domestic		Cross-border within EEA		Cross-border outside EEA	
		By volume	By value	By volume	By value	By volume	By value	By volume	By value	By volume	By value	By volume	By value
190	Total money remittances												

Payment initiation services

		A	B	C	D	E	F	G	H	I	J	K	L
		Geo breakdown for sent transactions						Geo breakdown for sent fraudulent transactions					
		Domestic		Cross-border within EEA		Cross-border outside EEA		Domestic		Cross-border within EEA		Cross-border outside EEA	
		By volume	By value	By volume	By value	By volume	By value	By volume	By value	By volume	By value	By volume	By value
191	Total payment initiation services												
	of which broken down by payment initiation channel												
192	Remote												
	of which broken down by authentication method (applicable only to PISPs issuing their own credentials and for the Authentication performed on these credentials):												
193	Authenticated via Strong Customer Authentication												
194	Authenticated via non-Strong Customer Authentication												
195	Non-remote												
	of which broken down by authentication method (applicable only to PISPs issuing their own credentials and for the Authentication performed on these credentials):												
196	Authenticated via Strong Customer Authentication												
197	Authenticated via non-Strong Customer Authentication												
	of which broken down by payment initiation channel												
198	Credit transfers												
199	Other												

Cash Withdrawals

		A	B	C	D	E	F	G	H	I	J	K	L
		Geo breakdown for sent transactions						Geo breakdown for sent fraudulent transactions					
		Domestic		Cross-border within EEA		Cross-border outside EEA		Domestic		Cross-border within EEA		Cross-border outside EEA	
		By volume	By value	By volume	By value	By volume	By value	By volume	By value	By volume	By value	By volume	By value
200	Total cash withdrawals												
	of which broken down by card function:												
201	Payments with cards with a debit function												
202	Payments with cards with a credit or delayed debit function												
	of which fraudulent card payments by fraud types:												
203	Issuance of a payment order by a fraudster												
	of which broken down by fraud sub-types:												
204	Lost or Stolen card												
205	Card Not Received												
206	Counterfeit card												
207	Card details theft												
208	Other												
209	Modification of a payment order by the fraudster												
210	Manipulation of the payer to make a card payment												

Losses borne due to fraud per liability bearer:

211	The reporting PSP												
212	The Payment Service User (payee)												
213	Others												

Table 2 - Fraud relating to account information services

	A	B	C
	Number of incidents of fraud	Total value of fraud across all incidents (or an estimation of the loss to the persons defrauded(£))	Please provide a brief description of how fraud was most commonly committed - descriptions of up to three different fraud types, in order of those with the highest loss
214	In respect of account information services only, please indicate:		
215			
216			

SUP 16 Annex 27F is deleted in its entirety and replaced. The new text is not underlined.

16 Annex 27F G Notes on completing REP017 Payments Fraud Report

These notes contain guidance for payment service providers that are required to complete the Payments Fraud Report in accordance with Regulation 109(4) of the Payment Services Regulations 2017, SUP 16.13.7D and the EBA Guidelines on fraud reporting under the Second Payment Services Directive (PSD2) ("the EBA Guidelines").

The following completion notes should be read in conjunction with the EBA Guidelines.

The form provides the means for PSPs to provide the FCA with statistical data on fraud related to different means of payment. In turn, the FCA is required to aggregate this data and share it with the EBA and the ECB.

As outlined in Guideline 1 of the EBA Guidelines, PSPs will be required to collect and submit data on the volume and value of all payment transactions, as well as the volume and value of fraudulent transactions.

Data on volume and value need to be broken down further by payment type, fraud type, method of authentication and geographical location. The detailed breakdown of data to be reported generally pertains only to the volume and value of fraudulent transactions (as opposed to all payment transactions). The EBA Guidelines explain these in detail. The following completion notes should be read as complementary to the Guidelines.

What is a fraudulent transaction?

For the purposes of this report, a fraudulent transaction is any payment transaction that the PSP has:

- executed;
- acquired; or
- in the case of a PISP, initiated;

and that the PSP deems to fall into either of the following categories:

a. 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'); and

b. 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 ('manipulation of the payer').

If a payment transaction meets the conditions above it should be recorded as a fraudulent transaction for the purposes of this report irrespective of whether:

- the PSP had primary liability to the user;
- the fraudulent transaction would be reported as such by another PSP in the same payment chain.

PSPs that provide account information services (AISPs) should have regard to the guidance in Table 2 below. Registered account information service providers (i.e. PSPs that do not provide any other type of payment service) do not need to answer the questions in Table 1.

Fraud committed by the payment service user should not be reported.

The payment service provider should not report data on payment transactions that, however linked to any of the circumstances referred to in the definition of fraudulent transaction (EBA Guideline 1.1), have not been executed and have not resulted in a transfer of funds in accordance with PSD2 provisions.

Structure of the return

In summary, REP017 requires the PSP to report the following fraud types, divided into sections for different payment and e-money services:

(for credit transfers)

- Issuance of a payment order by the fraudster.
- Modification of a payment order by the fraudster
- Manipulation of the payer by the fraudster to issue a payment order.

(for direct debits where consent is given via an electronic mandate or separately where consent is given in another form)

- Unauthorised payment transactions
- Manipulation of the payer by the fraudster to consent to a direct debit

(debit card transactions and separately for credit card transactions)

- Issuance of a payment order by the fraudster, broken down into:
    - Lost or stolen card
    - Card not received
    - Counterfeit card
    - Card details theft
    - Other
- Modification of a payment order by the fraudster
- Manipulation of the payer to make a card payment

(for e-money transactions – to be reported by e-money issuers)

- Issuance of a payment order by the fraudster, broken down into:
    - Lost or stolen card

    - Card not received
    - Counterfeit Card
    - Card details theft
    - Other
- Modification of a payment order by the fraudster
- Manipulation of the payer by the fraudster to issue a payment order

(for money remittance)

- Fraudulent payment transactions

(transactions initiated by payment initiations service providers (PISPs))

- Fraudulent payment transactions

(cash withdrawals)

- Issuance of a payment order by a fraudster refers to the following types of unauthorised card payment transactions, broken down into:
    - Lost or stolen card
    - Card not received
    - Counterfeit card
    - Other
- Manipulation of the payer to make a cash withdrawal

Fraud types

Below we provide guidance on the fraud types referred to in REP017. We give examples of these fraud types in relation to each payment or e-money service. PSPs should use their discretion when determining the appropriate fraud type for each fraudulent transaction and should choose the fraud type that most closely matches the circumstances of the fraud.

Credit transfers

Issuance of a payment order by the fraudster

This would cover unauthorised payment transactions where the fraudster uses stolen personalised security credentials in order to issue a payment order, either through contacting the victim's bank or accessing the victim's online banking service. For example, where a victim's online banking has been accessed using stolen personal identity details and credit transfers (such as Faster Payment or CHAPS payments) have been made or direct debits set up from the victim's account to beneficiaries chosen by the fraudster.

Modification of a payment order by the fraudster (credit transfers)

This would cover unauthorised payment transactions where the fraudster has gained unauthorised access to the victim's account in order to change the details of existing payment orders or payment instructions. For example, where a victim's account has been accessed using stolen personalised security credentials in order to modify the beneficiary of the victim's existing standing orders or direct debits or, for example, where a victim's account

has been accessed by a fraudster and a batch of payment details have been modified so that when payments are executed by the victim, the funds are unintentionally transferred to a beneficiary or beneficiaries chosen by the fraudster rather than the intended beneficiary. (See CIFAS paper, Table 2 Unlawful obtaining or disclosure of personal data: https://www2.cipd.co.uk/NR/rdonlyres/710B0AB0-ED44-4BD7-A527-B9AC29B28343/0/empfraud.pdf)

Manipulation of the payer by the fraudster to issue a payment order

This would cover fraud where the payer authorises a push payment to an account the payer believes belongs to a legitimate payee, however, the payer has been deceived into inputting the sort code and account number (or other unique identifier) of a fraudster, or an account controlled by a fraudster. This is also referred to as 'malicious misdirection'. For example, a scammer may contact a victim purporting to be from the victim's bank. The scammer may then convince the victim to transfer money (using a credit transfer) to a different account, purportedly in order to safeguard it. However, that account is in fact controlled by the scammer. (See Payment Systems Regulator response to Which? Super-complaint: https://www.psr.org.uk/psr-publications/news-announcements/which-super-complaint-our-response-Dec-2016).

Direct debits

Unauthorised transactions

This would cover fraud where a fraudster has set up a direct debit mandate in the name of a fraud victim and unauthorised direct debit payments are taken from the account of the victim.

Manipulation of the payer by the fraudster to consent to a direct debit

This would cover fraud where a fraudster **convinces a victim to change a direct debit. For example, the fraudster may purport to be an organisation the victim makes regular direct debit payments to, such as a subscription or membership organisation or business supplier. They may then convince the victim to change the direct debit to make payments to an account the fraudster owns or controls. (See Action Fraud** https://www.actionfraud.police.uk/mandate-fraud**)**

Debit and credit cards:

Issuance of a payment order by a fraudster

Refers to the following types of unauthorised card payment transactions:

'Lost or stolen card fraud'

This would cover any payment fraud committed as a result of a lost or stolen card (except where 'card not received fraud' has occurred). (See FFAUK Fraud Facts 2016 https://www.financialfraudaction.org.uk/fraudfacts16/assets/fraud_the_facts.pdf)

‘Card not received fraud’

This would cover fraud where a payment card is stolen (with or without the details of the PIN also being intercepted) whilst in transit – after the card company sends it out and before the genuine cardholder receives it. The payment card is then used by the fraudster to make transactions. (See FFAUK Fraud Facts 2016 https://www.financialfraudaction.org.uk/fraudfacts16/assets/fraud_the_facts.pdf)

‘Counterfeit card fraud’

This would cover fraud where the fraudster uses a card which has been printed, embossed or encoded so as to purport to be a legitimate card but which is not genuine because the issuer did not authorise the printing, embossing or encoding. (See https://www.financialfraudaction.org.uk/wp-content/uploads/2016/07/Fraud-the-Facts-A5-final.pdf)

‘Card details theft (card not present fraud)’

This would cover fraud where card details have been fraudulently obtained through methods such as unsolicited emails or telephone calls or digital attacks such as malware and data hacks, or card details being taken down from the physical card by a fraudster. The card details are then used to undertake fraudulent purchases over the internet, by phone or by mail order. It is also known as ‘card-not-present’ (CNP) fraud. (See https://www.financialfraudaction.org.uk/fraudfacts16/)

‘Other’

Unauthorised transactions relating to other types of fraud should be recorded under ‘other’.

Modification of a payment order by the fraudster (debit and credit card payments)

This is a type of unauthorised transaction and refers to a situation where the fraudster intercepts and modifies a legitimate payment order at some point during the electronic communication between the payer’s device (e.g. payment card) and the payment service provider (for instance through malware or attacks allowing attackers to eavesdrop on the communication between two legitimately communicating hosts (man in the middle attacks)) or modifies the payment instruction in the payment service provider’s system before the payment order is cleared and settled.

Manipulation of the payer to make a card payment

This would cover card payments that have been authorised by the payer, i.e. using chip and pin, or authenticated online card payments. The customer believes they are paying a legitimate payee, i.e. a merchant, but the payee that receives the funds is not a merchant, but instead a fraudster.

E-money transactions

The same fraud types apply to payment transactions involving e-money.

Money remittance and payment initiation services

Fraudulent transactions

Money remitters and PISPs are required under the EBA Guidelines to report 'fraudulent transactions'. Money remitters and PISPs should use their discretion when determining what to count as a 'fraudulent transaction'. Where money remitters or PISPs detect the frauds described above, these should be counted as 'fraudulent transactions'.

Cash withdrawals

Issuance of a payment order by a fraudster

This refers to the following types of unauthorised cash withdrawals at ATMs, at bank counters and through retailers ('cash back') using a card (or using a mobile app in place of a card):

- Those resulting from a lost or stolen payment card
- Those resulting from a payment card being stolen (with or without the details of the PIN also being intercepted) whilst in transit – after the card company sends it out and before the genuine cardholder receives it
- Those where the fraudster uses a card to withdraw money which has been printed, embossed or encoded so as to purport to be a legitimate card but which is not genuine because the issuer did not authorise the printing, embossing or encoding

Manipulation of the payer to make a cash withdrawal

This refers to reported frauds where a payment service user has withdrawn cash under duress or through manipulation.

Authentication method

For all credit transfers, card transactions and e-money transactions reported, the PSP should report whether strong customer authentication has been used or not. Strong customer authentication means authentication based on the use of two or more elements that are independent, in that the breach of one element does not compromise the reliability of any other element, and designed in such a way as to protect the confidentiality of the authentication data, with the elements falling into two or more of the following categories—

(a) something known only by the payment service user ('knowledge');

(b) something held only by the payment service user ('possession');

(c) something inherent to the payment service user ('inherence').

Where strong customer authentication is not used, the PSP should report under which of the following exemptions the transactions have taken place. These exemptions and their application are determined in the regulatory technical standards for strong customer

authentication and common and secure open standards of communication (SCA-RTS). As noted in the FCA Approach Document, "The exemptions are separate and independent from one another. Where a payment transaction may qualify for an exemption under several different categories (e.g. a low-value transaction at an unattended card 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." (paragraph 20.39).

For the purposes of reporting, the applicable exclusions are:

- Unattended terminal for transport or parking fares (Article 12 SCA-RTS)
- Trusted beneficiary (Article 13 SCA-RTS)
- Recurring transaction (Article 14 SCA-RTS)
- Low value (Article 16 SCA-RTS)
- Use of secure corporate payment processes or protocols (Article 17 SCA-RTS)
- Transaction risk analysis (Article18 SCA-RTS)

Losses borne due to fraud per liability bearer

PSPs are required to report the general value of losses borne by them and by the relevant payment service user, not net fraud figures.

The figure that should be reported as 'losses borne' is understood as the residual loss that is finally registered in the PSP's books after any recovery of funds has taken place. The final fraud losses should be reported in the period when they are recorded in the payment service provider's books.

We expect one single figure for any given period, unrelated to the payment transactions reported during that period.

Since refunds by insurance agencies are not related to fraud prevention for the purposes of PSD2, the final fraud loss figures should not take into account such refunds.

Data elements

<table>
<tr><td colspan="2">Payments Fraud Report – Table 1

Value should be reported in pounds sterling throughout (£)</td></tr>
<tr><td colspan="2">Totals: Transaction and fraudulent transaction volume and value for all payment types</td></tr>
<tr><td>1A – 1L
37A – 37L
47A – 47L
104A – 104L
159A – 159L
190A – 190L
191A – 191L</td><td>PSPs should report the following information in respect of the payment type – e.g. credit transfers, direct debits etc:

• Total domestic transaction volume (i.e. the number of transactions) for payment type – Column A</td></tr>
</table>

200A – 200L	• Total domestic transaction value for payment type Column B • Total transaction volume for payments made cross-border within the EEA – Column C • Total transaction value for payments made cross-border within the EEA – Column D • Total transaction volume for payments made cross-border outside the EEA – Column E • Total transaction value for payments made cross-border outside the EEA – Column F • Fraudulent transaction volume (i.e. the number of transactions) for payment type • Total domestic fraudulent transaction volume (i.e. the number of transactions) for payment type – Column G • Total domestic fraudulent transaction value for payment type Column H • Total fraudulent transaction volume for payments made cross-border within the EEA – Column I • Total fraudulent transaction value for payments made cross-border within the EEA – Column J • Total fraudulent transaction volume for payments made cross-border outside the EEA – Column K • Total fraudulent transaction value for payments made cross-border outside the EEA – Column L
The above reporting pattern for columns A-L is repeated for all subsequent rows, except: 54 – 61A to 54 – 61F 63 – 70A to 63 – 70F 80 – 87A to 80 – 87F 89 – 96A to 89 – 96F 101 – 103A to 101 – 103F 111 – 118A to 111 – 118F 120 – 127A to 120 – 127F 135 – 142A to 135 – 142F 144 – 151A to 144 – 151F 156 – 158A to 156 – 158F 162 – 164A to 162 – 164F 166 – 168A to 166 – 168F 176 – 178A to 176 – 178F 180 – 182A to 180 – 182F 197 – 199A to 197 – 199F 203 – 213A to 203 – 213F	
Payment initiation channel – initiated non-electronically	
2A – 2L 48A – 48L (card issuers)	Of the Total Transactions and Total Fraudulent Transaction volumes and values for **credit transfers** and **card payments**

105A – 105L (card acquirers)	**only**, PSPs should report the volume and value of those initiated non-electronically. Transactions initiated non-electronically include payment transactions initiated and executed with modalities other than the use of electronic platforms or devices. This includes paper-based payment transactions, mail orders or telephone orders (Recital 95 of the revised Payment Services Directive).
Payment initiation channel – initiated electronically	
3A – 3L 49A – 49L 106A – 106L	Of the Total Transactions and Total Fraudulent Transaction volumes and values for **credit transfers** and **card payments only**, PSPs should report the volume and value of those initiated electronically.
Remote transactions	
4A – 4L 50A – 50L 107A – 107L 160A – 160L	Of the Total Transactions and Total Fraudulent Transaction volumes and values for **credit transfers**, **card payments** and **E-money payment transactions only** PSPs should report the volume and value of those that are remote transactions. A 'remote transaction' means a payment transaction initiated via internet or through a device that can be used for distance communication (Revised Payment Services Directive Article 4(1)(6)).
Non-remote transactions	
19A – 19L 76A – 76L 131A – 131L	Of the Total Transactions and Total Fraudulent Transaction volumes and values for **credit transfers**, **card payments** and **E-money payment transactions only** PSPs should report the volume and value of those that are non-remote transactions. 'Non-remote' means any payment transactions that are not initiated via internet or through a device that can be used for distance communication.
Credit and debit card transactions	
51A – 51L 52A – 52L	For the total remote and total non-remote card transactions, PSPs should report the volumes and values that were credit card (including charge card) transactions and the volumes and values that were debit card transactions.
Strong customer authentication for credit transfers and card transactions	
5A – 5L (SCA) 9A – 9L (non-SCA) 20A – 20L (SCA) 24A – 24L (non-SCA)	For total remote and total non-remote credit transfers and card transactions, PSPs should report the volumes and values of sent and fraudulent transactions authenticated via strong

53A – 53L (SCA) 62A – 62L (non-SCA)	customer authentication and via non-strong customer authentication
Fraud types for credit transfers and card transactions	
6 – 8G to 6 – 8L 10 – 12G to 10 – 12L 21 – 23G to 21 – 23L	For remote transactions that were authenticated via strong customer authentication and non-strong customer authentication, PSPs should record the fraudulent transactions under the relevant fraud type (see guidance above). The same should be done for non-remote transactions.
Fraudulent transactions broken down by exemption from SCA for credit transfers and card transactions	
	Of the transactions authenticated without strong customer authentication, PSPs should provide the fraudulent transaction volumes and values, broken down by which exemption was used as per guidance above.

Fraud relating to account information services – Table 2		
Number of incidents of fraud		
214A	Please indicate the number of incidents of fraud.	This should be the total number of incidents of fraud that the AISP has recorded. If there are no incidents of fraud, please enter '0' (there is no need to complete the rest of Table 2).
Total value of fraud across all incidents (or an estimation of the loss to the persons defrauded (£))		
214B	Total value of fraud	Where known, the AISP should report the value of any fraudulent transactions that were executed or initiated (by a third party PSP) as a result of the fraud committed against the AIS user or the AISP. In all other circumstances the AISP should provide an estimation of the loss to the persons defrauded. In this context 'persons' would include the user of the AIS service, any other PSP (such as a credit institution that operated the payment account that the AISP accessed) or the AISP itself. 'Loss' would include loss of funds incurred as a result of fraudulent transactions or loss incurred as an indirect result of the fraud; for example by having to reissue new payment instruments or fix breached security systems.

		If the fraudulent incident(s) did not result in any financial loss, the AISP should still report the incident, enter '0' at 214B and explain the type of fraud at 214C. AISPs should convert values for non-sterling transactions into sterling using the average ECB reference exchange rate for the applicable reporting period, where available. In other instances AISPs should use the average of the applicable daily spot rate on the Bank of England's Statistical Interactive Database for the applicable reporting period.
Description of fraud		
214C – 216C	Description of fraud	In this section we would expect AISPs to describe the type of fraud that has resulted in the highest total value of fraud (unless the AISP is reporting fraudulent incidents that did not result in any financial losses, as above). The AISP should also explain how the losses were incurred (on the basis that the AISP does not come into possession of the payment transaction funds and is not responsible for the execution of payment transactions).

Part 3. Comes into force on 14 September 2019.

15	**Notifications to the FCA**		
15.1	**Application**		
…			
15.14	**Notifications under the Payment Services Regulations**		
…			
	Notification that a fraud rate has been exceeded (Article 20 of the SCA RTS)		
15.14.29	G	Article 18 of the *SCA RTS* permits *payment service providers* not to apply strong customer authentication where the payer initiates a remote electronic payment transaction identified by the *payment service provider* as posing a low level of risk according to the transaction monitoring mechanism referred to in Article 2 and Article 18 of the *SCA RTS*.	
15.14.30	G	Article 19 of the *SCA RTS* requires *payment service providers* to ensure that the overall fraud rates for transactions executed under the Article 18 exemption are equivalent to or lower than the reference fraud rates indicated in the Annex to the *SCA RTS*.	
15.14.31	G	Where a fraud rate calculated in compliance with Article 19 of the *SCA RTS* exceeds the applicable reference fraud rate, Article 20(1) of the *SCA RTS* requires *payment service providers* to immediately report to the *FCA*, providing a description of the measures that they intend to adopt to restore compliance with the reference fraud rates.	
15.14.32	G	*Payment service providers* should report in respect of each quarter in which a fraud rate exceeds the applicable reference rate.	
15.14.33	G	Where a fraud rate exceeds the applicable reference rate for two consecutive quarters, the *payment service provider* is required by Article 20(2) of the *SCA RTS* to immediately cease to make use of the Article 18 exemption. The report for the second quarter should confirm that the *payment service provider* has ceased to make use of the Article 18 exemption.	
15.14.34	D	*Payment service providers* required by Article 20(1) of the *SCA RTS* to report to the *FCA* must do so:	
		(1)	in the form specified in *SUP* 15 Annex 12;
		(2)	by electronic means made available by the *FCA*; and

		(3)	immediately after the monitored fraud rate exceeds the applicable reference fraud rate.
15.14.35	D	A *payment service provider* that has previously reported to the *FCA* in accordance with *SUP* 15.14.34D must notify the *FCA* in accordance with Article 20(4) of the *SCA RTS* before again making use of the Article 18 exemption:	
		(1)	in the form specified in *SUP* 15 Annex 12;
		(2)	by electronic means made available by the *FCA*; and
		(3)	in a reasonable timeframe and before making use again of the Article 18 exemption.
15.14.36	G	A *payment service provider* notifying the *FCA* before again making use of the Article 18 exemption must provide evidence of the restoration of compliance of their monitored fraud rate with the applicable reference fraud rate for that exemption threshold range for one quarter, under Article 20(4) of the *SCA RTS*.	
15.14.37	G	Notifying the *FCA* one month before making use again of the Article 18 exemption would be a reasonable timeframe within the meaning of *SUP* 15.14.35D(3).	
	Notifying problems with a dedicated interface (Article 33(3) of the SCA RTS)		
15.14.38	D	*Account information service providers*, *payment initiation service providers* and *account servicing payment service providers* must report problems with dedicated interfaces as required by Article 33(3) of the *SCA RTS* to the *FCA*:	
		(a)	without undue delay;
		(b)	using the form set out in *SUP* 16 Annex 13; and
		(c)	by electronic means made available by the *FCA*.
15.14.39	G	The following problems with dedicated interfaces should be reported:	
		(a)	the interface does not perform in compliance with Article 32 of the *SCA RTS*; or
		(b)	there is unplanned unavailability of the interface or a systems breakdown.
		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.	

15 Annex 12	D	Form NOT004 Notification that the fraud rate exceeds the reference fraud rate under SCA-RTS Article 20

NOT004 - Notification that the fraud rate exceeds the reference fraud rate under SCA-RTS Article 20

	Name of service provider			
	FRN			
	Details of the person the FCA should contact in relation to this notification: Title First names Surname Position Phone number (including STD code) Email address			
Q1	Is this a notification that one or more monitored fraud rates for remote electronic card-based payments or remote electronic credit transfers exceeds the applicable reference fraud rate?	[ ] Yes Continue to question 2 [ ] No If this is a notification that you intend to make use again of the transaction risk analysis exemption, go to question 8		
Q2	If this notification is not the first, please provide the reference number received when the original notification was submitted			
	Notification that the reference fraud rate is exceeded			
Q3	Please confirm that the fraud rates were calculated in accordance with SCA-RTS Article 19	[ ] Y [ ] N		
Q4	Please provide the PSP's fraud rate(s), where they exceed the applicable reference fraud rate		Remote electronic card-based payments	Remote electronic credit transfers
		EUR 500		
		EUR 250		
		EUR 100		
Q5	For how many consecutive quarters has the fraud rate exceeded the applicable reference rate (if more than 1 quarter, please continue to question 6; otherwise, go to question 7)?		Remote electronic card-based payments	Remote electronic credit transfers
		EUR 500		
		EUR 250		
		EUR 100		
Q6	Please provide the date on which the PSP ceased to apply the transactional risk analysis exemption for the type(s) of transaction which exceeded the applicable reference fraud rate (DD/MM/YYYY)		Remote electronic card-based payments	Remote electronic credit transfers
		EUR 500		
		EUR 250		
		EUR 100		
Q7	Please provide a description of the measures that the PSP intends to adopt to restore compliance of their monitored fraud rate(s) with the applicable reference fraud rate(s)	max 500 words		
	Notification that you intend to make use again of the transaction risk analysis exemption			

Q8	Please provide the PSP's fraud rate(s) from the last quarter that have been restored to compliance with the applicable reference fraud rate.		Remote electronic card-based payments	Remote electronic credit transfers
		EUR 500		
		EUR 250		
		EUR 100		
Q9	Please confirm that you have provided, alongside this notification, the underlying data and the calculation methodology used in relation to the fraud rate(s) that have been restored to compliance with the applicable reference fraud rate.	[ ] Y [ ] N		
Q10	When do you intend to start making use again of the transaction risk analysis exemption?	DD/MM/YYYY		

15 Annex 13	**D**	**Form NOT005 Notification that there are problems with a dedicated interface under SCA-RTS Article 33(3)**

NOT005 - Notification that there are problems with a dedicated interface under SCA-RTS Article 33(3)

	Name of service provider	
	FRN	
	Details of the person the FCA should contact in relation to this notification: Title First names Surname Position Phone number (including STD code) Email address	
Q1	In what capacity is the firm notifying?	[ ] ASPSP [ ] PISP [ ] AISP [ ] CBPII
	Details of the problem with the dedicated interface	
Q2	Is this a notification that the dedicated interface does not comply with SCA-RTS Article 32?	[ ] Yes Continue to question 3 [ ] No If this is a notification of unplanned unavailability or a systems breakdown, go to question 4
Q3	In what way is the dedicated interface failing to comply with Article 32? (select the option which best describes the problem)	[ ] The uptime of the dedicated interface, as measured by the key performance indicators described in Guidelines 2.2 and 2.4 of the EBA Guidelines on the conditions to be met to benefit from an exemption from contingency measures under Article 33(6) of the SCA-RTS, falls below the uptime of the interface used by the ASPSP's payment service users. [ ] There isn't the same level of support offered to AISPs and PISPs using the ASPSP's dedicated interface, in comparison to the customer interface. [ ] The dedicated interface poses obstacles to the provision of payment initiation and account information services (see SCA-RTS Article 32(3) and the EBA Guidelines and Opinion).

		[ ] Other failure to comply with Article 32.
Q4	[Only complete if the answer to question 2 was no] What is the problem in relation to unplanned unavailability or a systems breakdown? (select the option which best describes the problem)	[ ] Unavailability after five consecutive requests of information on the initiation of the payment transaction and all information accessible to the account servicing payment service provider regarding the execution of the payment transaction. [ ] Unavailability after five consecutive requests of information from designated payment accounts and associated payment transactions made available to the payment service user when directly requesting access to the account information excluding sensitive payments data. [ ] Other unplanned unavailability or systems breakdown.
Q5	Please give a brief description of the failure to comply with Article 32 or the unplanned unavailability or systems breakdown	Max 500 words
Q6	Time and date when the problem began	
	Has the problem been resolved at the time of submitting this notification?	Yes/No

16	**Reporting requirements**	
…		
16.13	**Reporting under the Payment Services Regulations**	
…		
	Reporting requirement	
…		
	Operational and Security Risk assessments	
…		
16.13.18	G	Article 17 of the *SCA RTS* permits *payment service providers* not to apply strong customer authentication in respect of legal persons initiating electronic *payment transactions* through the use of dedicated payment processes or protocols that are only made available to *payers* who are not consumers, where the *FCA* is satisfied that those processes and protocols guarantee at least equivalent levels of security to those provided for by the *Payment Services Directive*.

16.13.19	D	*Payment service providers* making use of the exemption in Article 17 of the *SCA RTS* must include in the operational and security risk assessment submitted in accordance with *SUP* 16.13.13D:	
		(1)	a brief description of the *payment services* provided in reliance on this exemption; and
		(2)	a brief explanation of how the *payment service provider*'s processes and protocols achieve at least equivalent levels of security to those provided for by the *Payment Services Directive*.
16.13.20	G	*Payment service providers* should comply with *SUP* 16.13.19D each time they prepare and submit the operational and security risk assessment required by regulation 98(2) of the *Payment Services Regulations* in respect of a period in which they have made use of the exemption in Article 17 of the *SCA RTS*.	
16.13.21	G	*Payment service providers* that follow the guidance in paragraphs 20.55 to 20.60 of the *FCA's* Approach Document and comply with *SUP* 16.13.19D may make use of the Article 17 exemption on the basis that the *FCA* is satisfied with the levels of security of their processes and protocols, unless informed otherwise by the *FCA*.	
		Note: see https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf.	
	Reporting statistics on the availability and performance of a dedicated interface		
16.13.22	G	Article 32(4) of the *SCA RTS* requires *account servicing payment service providers* that opt to provide a dedicated interface under Article 31 of the *SCA RTS* to monitor the availability and performance of that interface. They must also publish on their website quarterly statistics on the availability and performance of the dedicated interface and of the interface used by its *payment services users*.	
16.13.23	D	*Account servicing payment service providers* shall submit to the *FCA* the quarterly statistics on the availability and performance of a dedicated interface that they are required by Article 32(4) of the *SCA RTS* to publish on their website:	
		(1)	within 1 month of every publication of such statistics on the *account servicing payment service provider's* website; and
		(2)	by electronic means made available by the *FCA*.

Annex C

Amendments to the Dispute Resolution: Complaints sourcebook (DISP)

In this Annex, underlining indicates new text and striking through indicates deleted text unless otherwise stated.

1 Treating complainants fairly

…

1 Annex 1AD R Electronic money and payment services complaints return form

…

Table 4

Complaints relating to alleged *authorised push payment fraud*

		A	B
		Total opened	Total closed
257	Complaints relating to alleged *authorised push payment fraud*		

…

1 Annex 1AA G Notes on completing electronic money and payment services complaints return form

Payment Services Complaints Return

…

Tables 1, 2, ~~and~~ 3 and 4

In Tables 1, 2, ~~and~~ 3 and 4 …

…

Contextualisation (Table 3)

…

Complaints relating to alleged *authorised push payment fraud* (Table 4)

Information on complaints relating to alleged *authorised push payment fraud* should be provided in Table 4. Data in this table should not be included in any

total complaint figures as these complaints should already be reported in the preceding tables under the appropriate product/service groupings (for example, under ‘Credit transfer’).

…

Annex D

Amendments to the Credit Unions sourcebook (CREDS)

In this Annex, underlining indicates new text and striking through indicates deleted text unless otherwise stated.

…

9 Complaints reporting rules for credit unions

…

9 Annex 1 R Credit union complaints return

…

Complaints relating to alleged *authorised push payment fraud* Section 5B

	Total opened	Total closed
Complaints relating to alleged *authorised push payment fraud*		

…

Notes on completing completion of this return

…

Section 5B – Complaints relating to alleged *authorised push payment fraud*

Information on complaints relating to alleged *authorised push payment fraud* should be provided in this section. Data in this section should not be included in any total complaint figures as these complaints should already be reported in the preceding sections under the appropriate product/service groupings (for example, under 'Banking and credit cards').

…

Annex E

Amendments to the Banking Conduct of Business sourcebook (BCOBS)

In this Annex, underlining indicates new text and striking through indicates deleted text.

5	**Post sale**	
…		
5.1	**Post sale requirements**	
…		
	Security of electronic payments	
…		
5.1.10B	G	Such procedures should include authentication procedures for the verification of the identity of the *banking customer* or the validity of the use of a particular *payment instrument*, proportionate to the risks involved. Where appropriate, *firms* may wish to consider the adoption of 'strong customer authentication', as defined in the *Payment Services Regulations*, and specified in regulatory technical standards adopted by the European Commission under Article 98 of the *Payment Services Directive* (the *SCA-RTS*). The *FCA* gives guidance on strong customer authentication in Chapter 20 of the *FCA*'s Approach Document.
		Note: see https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf.

Annex F

Amendments to the Perimeter Guidance manual (PERG)

In this Annex, underlining indicates new text and striking through indicates deleted text.

Part 1. Comes into force on 18 December 2018.

15	**Guidance on the scope of the Payment Services Regulations 2017**
…	
15.3	**Negative scope/exclusions**
Q25A	**When might we be providing an account information service?**
… More than one business may be involved in obtaining, processing and using payment account information to provide an online service to a customer. However, the business that requires authorisation or registration to provide the account information service is the one that provides consolidated account information to the payment service user (including through an agent) in line with the payment service user's request to that business. <u>An agent of an account information service provider cannot provide or purport to provide account information services in its own right. This means that if a firm (Firm A) (which may or may not be an account information service provider) passes data to another firm (Firm B), and Firm B uses that data to provide account information services to its customers, Firm B must be authorised or registered with permission to provide account information services. However, if Firm A is an account information service provider and Firm B is acting as Firm A's agent, it may present Firm A's account information service to users through its own platform: for example, its website or application. It must be clear to the customer that Firm B is acting as agent of Firm A, the principal. This may include, for example, using Firm A's branding within Firm B's application. Further, the agreement for the provision of account information services will be between the customer and Firm A, the principal.</u>	
…	
15.4	**Small payment institutions, agents and exempt bodies**
Q28.	**We only wish to be an agent. Do we need to apply to the FCA and/or PRA for registration?**
No. If your principal is a payment institution, it is its responsibility to register you as its agent. Assuming your principal is not an EEA firm, you are required to be registered on the Financial Services Register before you provide payment services. If your principal is an EEA firm, your principal will need to comply with the relevant Home State legislation relating to your appointment. You will not be able to provide payment services in the UK	

on behalf of an EEA firm unless it has also complied with the relevant requirements for the exercise of its passport rights.

You may act for more than one principal, but each principal must register you as its agent.

An agent can only provide its principal's payment services; the agent cannot provide or purport to provide the services in its own right. A person who behaves, or otherwise holds themselves out, in a manner which indicates (or which is reasonably likely to be understood as indicating) that they are a payment service provider is guilty of an offence under regulation 139 of the PSRs 2017. It must be clear to a customer that the agent is acting on behalf of the principal and the agreement to provide payment services will be between the principal and the customer.

…	
15.5	**Negative scope/exclusions**
…	
Q33A.	**We are an e-commerce platform that collects payments from buyers of goods and services and then remits the funds to the merchants who sell goods and services through us – do the regulations apply to us?**

…

If an e-commerce platform is providing payment services as a regular occupation or business activity and does not benefit from an exclusion or exemption, it will need to be authorised or registered by us.

An example of an e-commerce platform that is likely to need to be authorised or registered by the FCA is one that provides escrow services as a regular occupation or business activity. Escrow services generally involve a payment service consisting of the transfer of funds from a payer to a payee, with the platform holding the funds pending the payee's fulfilment of certain conditions or confirmation by the payer. It should be kept in mind that an escrow service may be a regular occupation or business activity of a platform even if it is provided as part of a package with other services. Escrow providers do not typically have the authority to negotiate or conclude the sale or purchase of goods or services on behalf of the payer or the payee, and in those circumstances would not fall within the exclusion for commercial agents.

40.	**Which types of payment card could fall within the so-called 'limited network' exclusion (see PERG 15, Annex 3, paragraph (k))?**
The 'limited network' exclusion forms part of a broader exclusion which applies to services based on specific payment instruments that can be used only in a limited way and -	
(a)	allow the holder to acquire goods or services only in the issuer's premises;
(b)	are issued by a professional issuer and allow the holder to acquire goods or services only within a limited network of service providers which have direct commercial agreements with the issuer;
(c)	may be used only to acquire a very limited range of goods or services; or
(d)	are valid only in a single EEA State, are provided at the request of an undertaking or a public sector entity, and are regulated by a national or regional public authority for specific social or tax purposes to acquire specific goods or services from suppliers which have a commercial agreement with the issuer.
As regards (a), examples of excluded instruments could include:	
	staff catering cards - reloadable cards for use in the employer's canteen or restaurant;
	tour operator cards - issued for use only within the tour operator's holiday village or other premises (for example, to pay for meals, drinks and sports activities);
	store cards – ~~for example, a 'closed-loop' gift card,~~ where the card can only be used at the issuer's premises or website (so where a store card is co-branded with a third party debit card or credit card issuer and can be used as a debit card or credit card outside the store, it will not benefit from this exclusion). <u>On the other hand, in our view, 'gift cards' where the issuer is a retailer and the gift card can only be used to obtain goods or services from that retailer are not payment instruments within the meaning of the PSRs 2017. This is because these basic gift cards do not initiate payment orders; payment for the goods or services is made by the customer to the retailer of the goods in advance, when the card is purchased from the retailer. Accordingly, this exclusion is not relevant to them.</u>
…	

Part 2. Comes into force on 14 September 2019.

15.7	**Transitional provisions**
Q47.	**[deleted] ~~We are a provider of account information and payment initiation services who was providing those services before 12 January 2016. Can we continue to provide those services after the PSRs 2017 come into force?~~**
~~Yes, initially. Providers of account information services and payment initiation services 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 without registration or authorisation until the EBA's Regulatory Technical Standards on strong customer authentication and common and secure communication apply. However, while provided in reliance on this transitional provision, those services will be treated under the PSRs 2017 as if they were not account information services or payment initiation services. More information can be found in Chapters 3 and 17 of our Approach Document.~~	

Pub ref: 005751

12 Endeavour Square London E20 1JN
Telephone: +44 (0)20 7066 1000
Website: www.fca.org.uk