PAYMENT SERVICES (AMENDMENT) INSTRUMENT 2018

Powers exercised

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 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); and

(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, part 3 of Annex B and part 2 of Annex F which come into force on 14 September 2019, and Annexes D and E which come into force on 1 July 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
Banking: Conduct of Business sourcebook (BCOBS)	Annex C
Dispute Resolution: Complaints sourcebook (DISP)	Annex D
Credit Unions sourcebook (CREDS)	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 (Amendment) Instrument 2018.

By order of the Board
13 December 2018

Annex A

Amendments to the Glossary of definitions

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

Insert the following new definition 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 open standards of communication.

Amend the following definition 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

After SUP 15B (Applications and notifications under the benchmarks regulation and powers over Miscellaneous BM persons) insert the following new chapter, SUP 15C. 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 1D 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 1D.

15C.2.3 G The *EBA* issued Guidelines on 4 December 2018 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 chapter 17 of the *FCA*'s Approach Document.

[**Note:** see https://eba.europa.eu/documents/10180/2250578/Final+Report+on+Guidelines+on+the+exemption+to+the+fall+back.pdf/4e3b9449-ecf9-4756-8006-cbbe74db6d03 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 1D, *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) 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 1D	**Form: Request for exemption from the obligation to set up a contingency mechanism**

Form: Request for exemption from the obligation to set up a contingency mechanism

Where a group of *account servicing payment service providers* (ASPSPs) operates the same dedicated interface across different banking brands, subsidiaries or products, we require a single request for that dedicated interface.

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

D1	Financial Registration Number (FRN):	
D2	Interface Name/Id (ASPSPs submitting a return should provide the name or ID used within the PSP to identify the interface being reported on)	

D3	If this is a single request for a dedicated interface operated across different banking brands, subsidiaries or products, please provide the names of the different banking brands, subsidiaries or products	
D4	If this is a request for one of a number of dedicated interfaces being operated across different banking brands, subsidiaries or products, please identify the group (e.g. banking group) and the brand, subsidiary or product which is the subject of this request	
D5	Contact person name	
D6	Contact role within organisation	
D7	Contact phone number	
D8	Contact email address	

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 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 https://eba.europa.eu/documents/10180/2250578/Final+Report+on+Guidelines+on+the+exemption+to+the+fall+back.pdf/4e3b9449-ecf9-4756-8006-cbbe74db6d03.]

Form A: exemption criteria

	Service level, availability and performance (EBA Guideline 2)	
Q1	Has the ASPSP defined service level targets for out of hours support, monitoring, contingency plans and maintenance for its dedicated interface that are at least as stringent as those for the interface(s) used by its own payment service users (EBA Guideline 2.1)?	
Q2	Has the ASPSP put in place measures to calculate and record performance and availability indicators, in line with EBA Guidelines 2.2 and 2.3?	
	Publication of statistics (EBA Guideline 3)	
Q3	Please set out the plan for the quarterly publication of daily statistics on the availability and performance of the dedicated interface and payment service user interface.	
	Stress testing (EBA Guideline 4)	
Q4	Please provide a summary of the results of stress tests undertaken.	
	Obstacles (EBA Guideline 5)	
Q5	Please describe the method(s) of carrying out the authentication procedure(s) of the payment service user that are supported by the dedicated interface	
	Redirection ☐ Confirm that supporting evidence has been provided	Summary of the authentication procedure Explanation of why the methods of carrying out the authentication procedure does not create obstacles
	Decoupled	Summary of the authentication procedure

	☐ Confirm that supporting evidence has been provided	Explanation of why the methods of carrying out the authentication procedure does not create obstacles
	Embedded ☐ Confirm that supporting evidence has been provided	Summary of the authentication procedure
		Explanation of why the methods of carrying out the authentication procedure does not create obstacles
	Other authentication method ☐ Confirm that supporting evidence has been provided	Summary of the authentication procedure
		Explanation of why the methods of carrying out the authentication procedure does not create obstacles
	Design and testing to the satisfaction of PSPs (EBA Guideline 6) – also complete Form B	
Q6	Please provide information on whether, and, if so, how the ASPSP has engaged with AISPs, PISPs and CBPIIs in the design and testing of the dedicated interface.	
Q7	Please provide the date (DD/MM/YYYY) from which the ASPSP has made available, at no charge, upon request, the documentation of the technical specification of the dedicated interface specifying a set of routines, protocols, and tools needed by AISPs, PISPs and CBPIIs to interoperate with the systems of the ASPSP.	

Q8	Please provide the date (**DD/MM/YYYY)** on which the ASPSP published a summary of the technical specification of the dedicated interface on its website and a web link.		
Q9	Please provide the date (**DD/MM/YYYY**) on which the testing facility became available for use by AISP, PISPs, CBPIIs (and those that have applied for the relevant authorisation).		
Q10	Please provide the number of different PISPs, CBPIIs, AISPs that have used the testing facility.	AISPs	
		CBPIIs	
		PISPs	
Q11	Please provide a summary of the results of the testing as required.		
	Wide usage of the interface (EBA Guideline 7)		
Q12	Please provide a description of the usage of the dedicated interface in a three month (or longer) period prior to submission of the exemption request.		
Q13	Describe the measures undertaken to ensure wide use of the dedicated interface by AISPs, PISPs, CBPIIs.		
	Resolution of problems (EBA Guideline 8)		
Q14	Please describe the systems or procedures in place for tracking, resolving and closing problems, particularly those reported by AISPs, PISPs, and CBPIIs.		
Q15	Please explain any problems, particularly those reported by AISPs, PISPs and CBPIIs, that have not been resolved in accordance with the service level targets defined under EBA Guideline 2.1.		

Form B: (EBA Guideline 6) design of the dedicated interface

		Column A	Column B	Column C
Article	**Requirement**	**Description of the functional and technical specifications that the ASPSP has implemented to meet this requirement.** **[Where relevant, also reference to the specific market initiative API specification used to meet this requirement and the results of conformance testing attesting compliance with the market initiative standard]**	**Summary of how the implementation of these specifications fulfils the requirements of PSD2, SCA-RTS and FCA Guidelines** **[Where relevant, any deviation from the specific market initiative API specification which has been designed to meet this requirement]**	**If not in place at the time of submission of the exemption request, when will the functionality be implemented to meet the requirement (must be before 14 September 2019).** **Has a plan for meeting the relevant requirements been submitted to the FCA alongside this form?**
PSD2 Article 67 SCA-RTS Article 30 RTS	Enabling AISPs to access the necessary data from payment accounts accessible online			
PSD2 Article 65 & 66 SCA-RTS Article 30	Enabling provision or availability to the PISP, immediately after receipt of the payment order, of all the information on the initiation of the payment transaction and all information accessible to the ASPSP regarding the execution of the payment transaction			
SCA-RTS	Conforming to (widely used) standard(s) of communication issued by international or European standardisation organisations			

Article 30(3)				
PSD2 Article 64(2) SCA-RTS Article 30(1)(c)	Allowing the payment service user to authorise and consent to a payment transaction via a PISP			
PSD2 Article 66(3)(b) and 67(2)(b)	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.			
PSD2 Article 65(2)(c), 66(2)(d) and 67(2)(c) SCA-RTS Article 30(1)(a) and 34	Enabling the identification of the AISP/PISP/CBPII and support eIDAS for certificates			
SCA-RTS Article 10(2)(b)	Allowing for no more than 90 days re-authentication for AISPs			

SCA-RTS Article 36(5)	Enabling the ASPSPs and AISPs to count the number of access requests during a given period			
SCA-RTS Article 30(4)	Allowing for a change control process			
PSD2 Article 64(2) and 80(2) and 80(4)	Allowing for the possibility for an initiated transaction to be cancelled in accordance with PSD2, including recurring transactions			
SCA-RTS Article 36(2)	Allowing for error messages explaining the reason for the unexpected event or error			
PSD2 Article 19(6)	Supporting access via technology service providers on behalf of authorised actors			
PSD2 Article 97(5) and SCA-RTS Article 30(2)	Allowing AISPs and PISPs to rely on all authentication procedures issued by the ASPSP to its customers			
PSD2 Article 67(2)(d) and 30 (1)(b) and SCA-	Enabling the AISP to access the same information as accessible to the payment servicer user in relation to their designated payment accounts and associated payment transactions			

RTS Article 36(1)(a)				
SCA-RTS Article 36(1)(c)	Enabling the ASPSP to send, upon request, an immediate confirmation yes/no to the PSP (PISP and CBPII) on whether there are funds available			
PSD2 Article 97(2) and SCA-RTS Article 5	Enabling the dynamic linking to a specific amount and payee, including batch payments			
SCA-RTS Articles 30(2), 32(3), 18(2)(c)(v) and (vi) and 18(3)	Enabling the ASPSP to apply the same exemptions from SCA for transactions initiated by PISPs as when the PSU interacts directly with the ASPSP			
SCA-RTS Article 4	Enabling strong customer authentication composed of two different elements			
SCA-RTS Articles 28 & 35	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			
PSD2 Article 97(3)	Ensuring security at transport and application level			

SCA-RTS Articles 30(2)(c) and 35				
PSD2 Article 97(3) SCA-RTS Articles 22, 35 and 3	Supporting the needs to mitigate the risk for fraud, have reliable and auditable exchanges and enable providers to monitor payment transactions			
SCA-RTS Article 29	Allowing for traceability			
SCA-RTS Article 32	Allowing for the ASPSP's dedicated interface to provide at least the same availability and performance as the user interface			

Part 2: Comes into force on 1 January 2019

Amend the following as shown.

16 Reporting requirements

…

16.13 Reporting under the Payment Services Regulations

…

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~~ D ~~The return set out in *SUP* 16 Annex 27ED must be provided to the *FCA* at least once per year. The first return should cover the period beginning on 13 January 2018 and ending on 31 December 2018 and should be submitted by 31 January 2019. Subsequent returns should cover consecutive reporting periods of one year beginning on 1 January and ending on 31 December each year and should be submitted within 1 *month* of the end of the reporting period.~~

(1) In the case of an *authorised payment institution*, an *authorised electronic money institution* or a *credit institution*:

(a) the return set out in *SUP* 16 Annex 27ED must be provided to the *FCA* every six *months*;

(b) returns must cover the reporting periods 1 January to 30 June and 1 July to 31 December; and

(c) returns must be submitted within two *months* of the end of each reporting period.

(2) In the case of a *small payment institution*, a *registered account information service provider* or a *small electronic money institution*:

(a) two returns set out in *SUP* 16 Annex 27ED must be provided to the *FCA* every twelve *months.* Each return must cover a six-*month* period;

(b) one return must cover the period 1 January to 30 June and the other return must cover the period 1 July to 31 December; and

(c) both returns must be submitted within two *months* of the end of the calendar year.

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) 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 https://eba.europa.eu/documents/10180/2281937/Guidelines+on+fraud+reporting+under+Article+96%286%29%20PSD2+%28EBA-GL-2018-05%29.pdf]

The form in SUP 16 Annex 27E is deleted in its entirety and replaced with the following new form. The text of the form is not underlined as new.

16 Annex 27ED REP017 Payments Fraud Report

This annex consists only of one of more forms. Firms are required to submit the returns using the electronic means made available by the FCA.

SUP 16 Annex 27ED

REP017 Payments Fraud Report

		A
1	Please select the period that the data in this return covers	

Table 1 - Payment transactions and fraudulent payment transactions for payment services

Credit transfers

		A	B	C	D	E	F	G	H	I	J	K	L
		Geographical breakdown for payment transactions						Geographical breakdown for fraudulent payment 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
2	Total credit transfers *of which:*												
3	Initiated by payment initiation service providers												
4	Initiated non-electronically												
5	Initiated electronically *of which:*												
6	**Initiated via remote payment channel** *of which:*												
7	**Authenticated via strong customer authentication** *of which fraudulent credit transfers by fraud types:*												
8	Issuance of a payment order by the fraudster												
9	Modification of a payment order by the fraudster												
10	Manipulation of the payer by the fraudster to issue a payment order												
11	**Authenticated via non-strong customer authentication** *of which fraudulent credit transfers by fraud types:*												
12	Issuance of a payment order by the fraudster												
13	Modification of a payment order by the fraudster												
14	Manipulation of the payer by the fraudster to issue a payment order												
	of which broken down by reason for not applying strong customer authentication												
15	Low value												
16	Payment to self												
17	Trusted beneficiary												
18	Recurring transaction												
19	Use of secure corporate payment processes or protocols												

20	Transaction risk analysis												
21	**Initiated via non-remote payment channel** *of which:*												
22	**Authenticated via strong customer authentication** *of which fraudulent credit transfers by fraud types:*												
23	Issuance of a payment order by the fraudster												
24	Modification of a payment order by the fraudster												
25	Manipulation of the payer by the fraudster to issue a payment order												
26	**Authenticated via non-strong customer authentication** *of which fraudulent credit transfers by fraud types:*												
27	Issuance of a payment order by the fraudster												
28	Modification of a payment order by the fraudster												
29	Manipulation of the payer by the fraudster to issue a payment order												
	of which broken down by reason for not applying strong customer authentication												
30	Payment to self												
31	Trusted beneficiary												
32	Recurring transaction												
33	Contactless low value												
34	Unattended terminal for transport or parking fares												

Losses due to fraud per liability bearer:

		A Total losses
35	The reporting payment service provider	
36	The Payment service user (payer)	
37	Others	

Direct debits

		A	B	C	D	E	F	G	H	I	J	K	L
		Geographical breakdown for payment transactions						Geographical breakdown for fraudulent payment 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
38	Total direct debits *of which:*												
39	**Consent given via an electronic mandate** *of which fraudulent direct debits by fraud type:*												

40	Unauthorised payment transactions											
41	Manipulation of the payer by the fraudster to consent to a direct debit											
42	**Consent given in another form than an electronic mandate**											
	of which fraudulent direct debits by fraud type:											
43	Unauthorised payment transactions											
44	Manipulation of the payer by the fraudster to consent to a direct debit											

Losses due to fraud per liability bearer:

		A Total losses
45	The reporting payment service provider	
46	The Payment service user (payer)	
47	Others	

Card payments (except cards with an e-money function only)

		A	B	C	D	E	F	G	H	I	J	K	L
		Geographical breakdown for payment transactions						Geographical breakdown for fraudulent payment 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
48	Total card payments (except cards with an e-money function only)												
	of which:												
49	Initiated non-electronically												
50	Initiated electronically												
	of which:												
51	**Initiated via remote payment channel**												
	of which broken down by card function:												
52	Payments with cards with a debit function												
53	Payments with cards with a credit or delayed debit function												
	of which:												
54	**Authenticated via strong customer authentication**												
	of which fraudulent card payments by fraud types:												
55	Issuance of a payment order by a fraudster												
	of which:												
56	Lost or stolen card												
57	Card not received												
58	Counterfeit card												
59	Card details theft												
60	Other												
61	Modification of a payment order by the fraudster												

62	Manipulation of the payer to make a card payment												
63	**Authenticated via non-strong customer authentication**												
	of which fraudulent card payments by fraud types:												
64	Issuance of a payment order by a fraudster												
	of which:												
65	Lost or stolen card												
66	Card not received												
67	Counterfeit card												
68	Card details theft												
69	Other												
70	Modification of a payment order by the fraudster												
71	Manipulation of the payer to make a card payment												
	of which broken down by reason for not applying strong customer authentication												
72	Low value												
73	Trusted beneficiary												
74	Recurring transaction												
75	Use of secure corporate payment processes or protocols												
76	Transaction risk analysis												
77	**Initiated via non-remote payment channel**												
	of which broken down by card function:												
78	Payments with cards with a debit function												
79	Payments with cards with a credit or delayed debit function												
	of which:												
80	**Authenticated via strong customer authentication**												
	of which fraudulent card payments by fraud types:												
81	Issuance of a payment order by a fraudster												
	of which:												
82	Lost or stolen card												
83	Card not received												
84	Counterfeit card												
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:												

90	Lost or stolen card											
91	Card not received											
92	Counterfeit card											
93	Other											
94	Modification of a payment order by the fraudster											
95	Manipulation of the payer to make a card payment											
	of which broken down by reason for not applying strong customer authentication											
96	Trusted beneficiary											
97	Recurring transaction											
98	Contactless low value											
99	Unattended terminal for transport or parking fares											

Losses due to fraud per liability bearer:

		A Total losses
100	The reporting payment service provider	
101	The Payment service user (payer)	
102	Others	

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

		A	B	C	D	E	F	G	H	I	J	K	L
		Geographical breakdown for payment transactions						Geographical breakdown for fraudulent payment 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
103	Total card payments acquired (except cards with an e-money function only) *of which:*												
104	Initiated non-electronically												
105	Initiated electronically *of which:*												
106	**Acquired via a remote channel** *of which broken down by card function:*												
107	Payments with cards with a debit function												
108	Payments with cards with a credit or delayed debit function												
	of which:												
109	**Authenticated via strong customer authentication** *of which fraudulent card payments by fraud types:*												
110	Issuance of a payment order by a fraudster *of which:*												

111	Lost or stolen card												
112	Card not received												
113	Counterfeit card												
114	Card details theft												
115	Other												
116	Modification of a payment order by the fraudster												
117	Manipulation of the payer to make a card payment												
118	**Authenticated via non-strong customer authentication** *of which fraudulent card payments by fraud types:*												
119	Issuance of a payment order by a fraudster *of which:*												
120	Lost or stolen card												
121	Card not received												
122	Counterfeit card												
123	Card details theft												
124	Other												
125	Modification of a payment order by the fraudster												
126	Manipulation of the payer to make a card payment												
	of which broken down by reason for not applying strong customer authentication												
127	Low value												
128	Recurring transaction												
129	Transaction risk analysis												
130	**Acquired via a non-remote channel** *of which broken down by card function:*												
131	Payments with cards with a debit function												
132	Payments with cards with a credit or delayed debit function												
	of which:												
133	**Authenticated via strong customer authentication** *of which fraudulent card payments by fraud types:*												
134	Issuance of a payment order by a fraudster *of which:*												
135	Lost or stolen card												
136	Card not received												
137	Counterfeit card												
138	Other												

139	Modification of a payment order by the fraudster											
140	Manipulation of the payer to make a card payment											
141	**Authenticated via non-strong customer authentication** *of which fraudulent card payments by fraud types:*											
142	Issuance of a payment order by a fraudster *of which:*											
143	Lost or stolen card											
144	Card not received											
145	Counterfeit card											
146	Other											
147	Modification of a payment order by the fraudster											
148	Manipulation of the payer to make a card payment											
	of which broken down by reason for not applying strong customer authentication											
149	Recurring transaction											
150	Contactless low value											
151	Unattended terminal for transport or parking fares											

Losses due to fraud per liability bearer:

		A Total losses
152	The reporting payment service provider	
153	The Payment service user (payer)	
154	Others	

Cash withdrawals

		A	B	C	D	E	F	G	H	I	J	K	L
		Geographical breakdown for payment transactions						Geographical breakdown for fraudulent payment 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
155	Total cash withdrawals *of which broken down by card function:*												
156	Payments with cards with a debit function												
157	Payments with cards with a credit or delayed debit function												

of which fraudulent card payments by fraud types:

158	Issuance of a payment order (cash withdrawal) by the fraudster						
	of which:						
159	Lost or stolen card						
160	Card not received						
161	Counterfeit card						
162	Other						
163	Manipulation of the payer to make a cash withdrawal						

Losses due to fraud per liability bearer:

		A Total losses
164	The reporting payment service provider	
165	The Payment service user (account holder)	
166	Others	

E-money payment transactions

		A	B	C	D	E	F	G	H	I	J	K	L
		Geographical breakdown for payment transactions						Geographical breakdown for fraudulent payment 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
167	Total e-money payment transactions												
	of which:												
168	**Via remote payment initiation channel**												
	of which:												
169	**Authenticated via strong customer authentication**												
	of which fraudulent credit transfers by fraud types:												
170	Issuance of a payment order by the fraudster												
171	Modification of a payment order by the fraudster												
172	Manipulation of the payer by the fraudster to issue a payment order												
173	**Authenticated via non-strong customer authentication**												
	of which fraudulent credit transfers by fraud types:												
174	Issuance of a payment order by the fraudster												
175	Modification of a payment order by the fraudster												
176	Manipulation of the payer by the fraudster to issue a payment order												
	of which broken down by reason for not applying strong customer authentication												
177	Low value												
178	Trusted beneficiary												
179	Recurring transaction												

180	Payment to self												
181	Use of secure corporate payment processes or protocols												
182	Transaction risk analysis												
183	**Via non-remote payment initiation channel** *of which:*												
184	**Authenticated via strong customer authentication** *of which fraudulent credit transfers by fraud types:*												
185	Issuance of a payment order by the fraudster												
186	Modification of a payment order by the fraudster												
187	Manipulation of the payer by the fraudster to issue a payment order												
188	**Authenticated via non-strong customer authentication** *of which fraudulent credit transfers by fraud types:*												
189	Issuance of a payment order by the fraudster												
190	Modification of a payment order by the fraudster												
191	Manipulation of the payer by the fraudster to issue a payment order												
	of which broken down by reason for not applying strong customer authentication												
192	Trusted beneficiary												
193	Recurring transaction												
194	Contactless low value												
195	Unattended terminal for transport or parking fares												

Losses due to fraud per liability bearer:

		A Total losses
196	The reporting payment service provider	
197	The Payment service user	
198	Others	

Money remittances

		A	B	C	D	E	F	G	H	I	J	K	L
		Geographical breakdown for payment transactions						Geographical breakdown for fraudulent payment 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
199	Total money remittances												

Payment transactions initiated by payment initiation service providers

	A	B	C	D	E	F	G	H	I	J	K	L
	Geographical breakdown for payment transactions						Geographical breakdown for fraudulent payment 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 payment transactions initiated by payment initiation service providers *of which:*												
201	**Initiated via remote payment channel** *of which:*												
202	Authenticated via Strong Customer Authentication												
203	Authenticated via non-Strong Customer Authentication												
204	**Initiated via non-remote payment channel** *of which:*												
205	Authenticated via Strong Customer Authentication												
206	Authenticated via non-Strong Customer Authentication												
	of which broken down by payment instrument												
207	Credit transfers												
208	Other												

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 commonly committed - descriptions of up to three different fraud types, in order of those with the highest loss
209	In respect of account information services only, please indicate			

The guidance notes in SUP 16 Annex 27F are deleted in their entirety and replaced with the below new notes. The text is not underlined.

16 Annex 27FG 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.

Question A1 – reporting period

As per SUP16.13.8, small payment institutions, registered account information service providers and small electronic money institutions must report once per year. All other PSPs must report every six months.

Those PSPs required to report annually are required to provide separate Payment Fraud Reports in respect of the two halves of the reporting year. These PSPs should use question 1 in the Payments Fraud Report to select the period the data in their return covers, e.g. "H1" for the period covering 1 January to 30 June, and "H2" for the period covering 1 July to 31 December.

Table 1 - Payment transactions and fraudulent payment transactions for payment services

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.

Table 2 - Fraud relating to account information services

PSPs that provide account information services (AISPs) should have regard to Table 2 in the fraud report (and 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 of the fraud report.

Adjustments

The date to be considered by PSPs for recording payment transactions and fraudulent payment transactions for the purpose of this statistical reporting is the day the transaction has been executed in accordance with PSD2.

However, payment service users are entitled to redress for unauthorised transactions as long as they have notified their PSP no later than 13 months after the debit date, on becoming aware of any unauthorised payment transactions. This means PSPs may need to adjust reports which they have already submitted, on becoming aware of fraudulent transactions executed in previous reporting periods.

Furthermore, the payment service provider should report all fraudulent payment transactions from the time fraud has been detected (i.e. because it has been reported to the PSP such as through a customer complaint or otherwise discovered independently by the PSP), regardless of whether or not the case related to the fraudulent payment transaction has been closed by the time the data are reported. This means PSPs may need to adjust reports which they have already submitted, should investigation of open fraud cases conclude that a transaction was not fraudulent.

PSPs should report adjustments during the next reporting window after the information necessitating the adjustment is discovered.

PSPs should make use of the resubmission facility made available via the electronic means for submitting REP017.

Table 1 - What is a fraudulent transaction?

For the purposes of table 1 a fraudulent transaction is any payment transaction that the PSP has:

- executed;
- acquired; or
- in the case of a payment initiation service provider (PISP), initiated;

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

- 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

- 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; or
- the fraudulent transaction would be reported as such by another PSP in the same payment chain.

As a general rule, for all types of payment services, the payer's PSP has to report, except for direct debit transactions, which are reported by the payee's PSP. In addition, card payments are reported both by the payer's PSP (the issuer) and the payee's PSP (the acquirer).

Fraud committed by the payment service user (known as first party fraud) 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.

The category of 'payment transactions made as a result of the payer being manipulated by the fraudster to issue a payment order' covers a broader range of payment types than what is known in the UK as 'authorised push payment fraud'. The latter is restricted to credit transfers authorised by the payer to a fraudster.

Table 1 - 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 (including those initiated by PISP):

- 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 a 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;

cash withdrawals:

- issuance of a payment order by the fraudster refers to the following types of unauthorised card payment transactions, broken down into:
    - lost or stolen card;
    - card not received;
    - counterfeit card;
    - other; and
- manipulation of the payer to make a cash withdrawal.

for e-money transactions – to be reported by e-money issuers:

- 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 money remittance:

- fraudulent payment transactions.

Table 1 - 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 covers unauthorised payment transactions in which 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 have been made from the victim's account to beneficiaries chosen by the fraudster.

Modification of a payment order by the fraudster

This covers 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. A victim's account could be accessed by a fraudster in order to modify a batch of payment details so that when payments are executed by the victim's PSP, 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 covers fraud where the payer authorises a push payment to an account the payer believes belongs to a legitimate payee, however, the payer was 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 payment transactions

This covers fraud where a victim's account details (e.g. sort code and account number) have been used by the fraudster to set up direct debit payments to an organisation, without the victim's knowledge or consent, resulting in unauthorised direct debit payments being taken from the account of the victim.

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

This covers fraud where a payer is convinced by a fraudster to set up a direct debit and consent to payments being made to an intended payee (the legitimate payee), but the fraudster uses the victim's details and consent to set up direct debit payments to a different (unintended) payee.

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 covers 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 covers 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 covers 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

This covers fraud where card details have been fraudulently obtained through methods such as unsolicited emails or telephone calls, 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.

Cash withdrawals

Issuance of a payment order by the fraudster

This refers to the following types of unauthorised cash withdrawals at ATMs, 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; and
- 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 under duress or through manipulation (using a card, or using a mobile app in place of a card).

E-money transactions

The same fraud types as above for debit and credit cards 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'.

Authentication method

For all credit transfers, card transactions and e-money transactions reported, including those initiated by PISP, 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—

- something known only by the payment service user ("knowledge");
- something held only by the payment service user ("possession"); or
- 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 Rik Analysis (article 18 SCA-RTS);

Data elements

Table 1 – Payment transactions and fraudulent payment transactions for payment services *Value should be reported in pounds sterling throughout (£)*	
Totals: Transaction and fraudulent transaction volume and value for all payment types	
Guide to the relevant area of the form	PSPs should report the following information in respect of the payment type – e.g. credit transfers, direct debits etc:
2A-2L 38A–38L 48A–48L 103A–103L 155A–155L 167A–167L 199A–199L 200A–200L	• total domestic transaction volume (i.e. the number of transactions) for payment type – Column A; • 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; • 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; and • 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 the following rows where only columns G to L are to be reported for the fraudulent transaction volume and value relating to the fraud type:

Credit transfers
8-10
12-14
23-25
27-29

Direct debits
40-41
43-44

Card payment (except cards with an e-money function only)
55-62
64-71
81-87
89-95

Card payment acquired (except cards with an e-money function only)
110-117
119-126
134-140
142-148

Cash withdrawals
158-163

E-money payment transactions 170-172 174-176 185-187 189-191	
Initiated by payment initiation service providers	
3A-3L	Of the total transaction and total fraudulent transaction volumes and values for **credit transfers**, PSPs should report the volume and value of those initiated by payment initiation service providers.
Payment initiation channel – initiated non-electronically	
4A–4L (credit transfers) 49A–49L (card payments) 104A-104L (card payments acquired)	Of the total transaction and total fraudulent transaction volumes and values for **credit transfers** and **card payments 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	
5A–5L (credit transfers) 50A–50L (card payments) 105A–105L (card payment acquired)	Of the total transaction 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	
6A-6L (credit transfers) 51A–51L (card payments) 106A–106L (card payments acquired) 168A–168L (e-money payment transactions)	Of the total transaction 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 the internet or through a device that can be used for distance communication (revised Payment Services Directive article 4(1)(6)).
Non-remote transactions	
21A–21L (credit transfers) 77A–77L (card payments)	Of the total transaction and total fraudulent transaction volumes and values for **credit transfers**, **card payments** and

130A–130L (card payments acquired) 183A–183L (e-money payment transactions)	**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 the internet or through a device that can be used for distance communication.
Credit and debit card transactions	
Card payments 52A–52L (remote > debit) 53A–53L (remote > credit) 78A–78L (non-remote > debit) 79A-79L (non-remote > credit) **Card payments acquired** 107A–107L (remote > debit) 108A–108L (remote > credit) 131A–131L (non-remote > debit) 132A–132L (non-remote > credit)	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	
Credit transfers 7A–7L (remote > SCA) 11A–11L (remote > non-SCA) 22A–22L (non-remote > SCA) 26A–26L (non-remote > non-SCA) **Card payments** 54A–54L (remote > SCA) 63A–63L (remote > non-SCA) 80A–80L (non-remote > SCA) 88A–88L (non-remote > non-SCA) **Card payments acquired** 109A–109L (remote > SCA) 118A–118L (remote > non-SCA 133A–133L (non-remote > SCA) 141A–141L (non-remote > non-SCA) **E-money payment transactions** 169A–169L (remote > SCA) 173A–173L (remote > non-SCA) 184A–184L (non-remote > SCA)	For total remote and total non-remote credit transfers, card transactions, e-money payment transactions and payment transactions initiated by payment initiation service providers, PSPs should report the volumes and values of sent and fraudulent transactions authenticated via strong customer authentication and via non-strong customer authentication

188A–188L (non-remote > non-SCA) **Payment transactions initiated by payment initiation service providers** 202A–202L (remote > SCA) 203A–203L (remote > non-SCA) 205A–205L (non-remote > SCA) 206A–206L (non-remote > non-SCA)	
Payment transactions initiated by payment initiation service providers	
207A–208L	Payment initiation providers reporting total transactions and total fraudulent transactions initiated, should report the value and volume of transactions that were credit transfers and the volume and value of other types of transactions that were using other payment instruments.
Fraud types	
Credit transfers 8–10 12–14 23–25 27–29 **Direct debits** 40–41 43–44 **Card payment (except cards with an e-money function only)** 55–62 64–71 81–87 89–95 **Card payment acquired (except cards with an e-money function only)** 110–117 119–126 134–140 142–148 **Cash withdrawals** 158–163 **E-money payment transactions**	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.

170–172 174–176 185–187 189–191	
Fraudulent transactions broken down by exemption from SCA	
Credit transfers 15A–20L 30A–34L **Card payments** 72A–76L 96A–99L **Card payments acquired** 127A–129L 149A–151L **E-money payment transactions** 177A–182L 192A–195L	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.
Losses due to fraud per liability bearer	
35A, 36A, 37A, 45A, 46A, 47A, 100A, 101A,102A, 152A, 153A, 154A	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.

Table 2 - Fraud relating to account information services		
Number of incidents of fraud		
209A	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 (£))		

209B	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' includes 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' includes loss of funds incurred as a result of fraudulent transactions and/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		
209C	Description of fraud	AISPs should describe the type of fraud that has resulted in the highest total value of fraud in this section (unless the AISP is reporting fraudulent incidents that did not result in any financial losses, as above). AISPs should also explain how the losses were incurred (on the basis that the AISP did not come into possession of the payment transaction funds and was not responsible for the execution of payment transactions).

Amend the following as shown.

TP 1 Transitional provisions

…

TP 1.2

(1)	(2) Material to which the transitional provision applies	(3)	(4) Transitional provision	(5) Transitional provision: dates in force	(6) Handbook provision: coming into force
…					
13B	…				
13C	*SUP* 16.13.7D	D	Statistical data on fraud covering the period beginning on 13 January 2018 and ending on 31 December 2018 must be submitted using the format of the return that would have been required to be submitted had *SUP* 16 Annex 27ED remained in the form in which it stood on 31 December 2018 and had *SUP* 16 not been amended by the Payment Services (Amendment) Instrument 2018. *SUP* 16 Annex 27ED, as it stood on 31 December 2018, and guidance notes for completion of this return can be accessed by using the timeline on the *FCA Handbook* website.	1 to 31 January 2019	1 January 2019
13D	*SUP* 16.13.8D	D	The return covering the period beginning on 13 January 2018 and ending on 31 December 2018 must be submitted by 31 January 2019.	1 to 31 January 2019	1 January 2019

13E	*SUP* 16.13.7D	D	In respect of the reporting period 1 January 2019 to 30 June 2019, the statistical data on fraud must be provided on a best endeavours basis. *Payment service providers* must provide at least the transaction and fraud totals that would have required to be collected had *SUP* 16 Annex 27ED remained in the form in which it stood on 31 December 2018 and had *SUP* 16 not been amended by the Payment Services (Amendment) Instrument 2018. *SUP* 16 Annex 27ED, as it stood on 31 December 2018, can be accessed by using the timeline on the *FCA Handbook* website.	1 January 2019 to 29 February 2020	1 January 2019
13F	*SUP* 16.13.7D	D	*Small payment institutions* may provide the statistical data on fraud in respect of 1 January 2019 to 30 June 2019 on a best endeavours basis. They must submit the data in respect of 1 July 2019 to 31 December 2019 in compliance with *SUP* 16.13.7D.	1 January 2019 to 29 February 2020	1 January 2019

Part 3: Comes into force on 14 September 2019

15 Notifications to the FCA

…

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 per quarter 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*. Article 19 defines a quarter as 90 *days*.

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 12D;

(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 ceased to make use of the article 18 exemption in accordance with article 20(2) of the *SCA RTS* 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 12D;

(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*, *payment service providers* issuing card-based *payment instruments*, 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 13R; 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.

After SUP 15 Annex 11D insert the following new Annexes. The text is not underlined.

15 Annex 12D 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 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	[ ] Yes [ ] No		
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.	[ ] Yes [ ] No		
Q10	When do you intend to start making use again of the transaction risk analysis exemption?	(DD/MM/YYYY)		

15 Annex 13D 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 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]	[ ] 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.

	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 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. [ ] Failure to provide to the card based payment instrument issuer (CBPII) or to the PISP a 'yes/no' confirmation in accordance with article 65(3) of PSD2 and article 36(1)(c) of the RTS. [ ] Other unplanned unavailability or systems breakdown.
Q5	Please give a brief description of the failure to comply with article 32 or the unplanned unavailability or systems breakdown. If an ASPSP, please provide the reason(s) for the problem and steps taken to resolve the issue.	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

Amend the following as shown.

16 Reporting requirements

…

16.13 Reporting under the Payment Services Regulations

…

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* intending to make 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 description of the *payment services* that the *payment service provider* intends to provide in reliance on this exemption; and

(2) an 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 D *Payment service providers* should comply with *SUP* 16.13.19D at least three *months* before making use of the exemption in article 17 of the *SCA RTS*, and subsequently 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 article 17 exemption.

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 and 16.13.20D 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 the quarter to which the statistics relate;

(2) using the form set out in *SUP* 16 Annex 46AD; and

(3) by electronic means made available by the *FCA*.

16.13.24 G The quarterly statistics should cover the periods January to March, April to June, July to September and October to December.

An *account servicing payment service provider* becoming subject to the obligation in *SUP* 16.13.23D part way through a quarter should submit the first statistics only in relation to the part of the quarter when this obligation applied.

Guidance notes for completing the form set out in *SUP* 16 Annex 46AD are in *SUP* 16 Annex 46BG.

…

16 Annex 27G REP018 Operational and Security risk reporting form

REP018 Operational and Security Risk	**A**
1 Are you submitting an operational and security risk report this quarter? If you answer 'No', Questions 2 to 9 do not need to be completed	
2 Date Assessment of the operational and security risks was performed	
3 Date Assessment of the adequacy of the mitigation measures and control mechanisms to mitigate Operational and Security risks was performed	
4 Were any deficiencies identified in the assessment of adequacy of mitigation measures?	
5 Summarise the deficiencies identified in question 4 (up to 400 characters - full details should be included in the attached report)	
6 Date of last audit of security measures	
7 Summary of issues identified in last audit of security measures (up to 400 characters - full details should be included in the attached report)	
8 Summary of action taken to mitigate any issues identified in question 7 (up to 400 characters - full details should be included in the attached report)	

9 Number of security related customer complaints to senior management during the reporting period.	
10 Are you applying the 'corporate payment exemption' under Article 17 of Commission Delegated Regulation (EU) 2018/389?	Y/N

16 Annex Notes on completing REP018 Operational and Security Risk form 27H

These notes contain *guidance* for *payment service providers* that are required to complete the operational and security risk form in accordance with regulation 98(2) of the *Payment Services Regulations* and *SUP* 16.13.13D. The *guidance* relates to the assessments that must be attached to the form in accordance with *SUP* 16.13.13D(2).

The *payment service provider* must attach to the form the latest:

- assessment of the operational and security risks related to the *payment services* the *firm* provides; and
- assessment of the adequacy of the mitigation measures and control mechanisms implemented in response to those risks.

The operational and security risk assessment should include all the requirements contained in the *EBA* Guidelines for operational and security risks of payment services as issued at 12 December 2017. These include:

- a list of business functions, processes and information assets supporting payment services provided and classified by their criticality;
- a risk assessment of functions, processes and assets against all known threats and vulnerabilities;
- a description of security measures to mitigate security and operational risks identified as a result of the above assessment; and
- conclusions of the results of the risk assessment and summary of actions required as a result of this assessment.

Payment service providers intending to make use of the exemption in article 17 of the *SCA RTS* must include:

- a description of the *payment services* that the *payment service provider* intends to provide in reliance on this exemption; and
- an 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*.

The assessment of the adequacy of mitigation measures and control mechanisms should include all the requirements contained in the *EBA* Guidelines for operational and security risks of payment services as issued at 12 December 2017. These include:

- a summary description of methodology used to assess effectiveness and adequacy of mitigation measures and control mechanisms;
- an assessment of the adequacy and effectiveness of mitigation measures and control mechanisms; and
- conclusions on any deficiencies identified as a result of the assessment and proposed corrective actions.

[**Note:** see https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2]

After SUP 16 Annex 45BG (Guidance notes for completion of the Annual Claims Management Report form) insert the following new Annexes. The text is not underlined.

16 Annex 46AD	**REP020 Statistics on the availability and performance of a dedicated interface**

REP020 Quarterly statistics on availability and performance of dedicated interfaces

		A
1	Do you wish to make a nil return?	

2 **Daily statistics**

This section must be completed for each payment service user interface and dedicated interface for which the firm has published the daily statistics on its website.

	A
Interface Name/Id	

	Availability statistics		Performance statistics				
			Payment services user interface	Dedicated interface			
	B						
	Interface type						
	C						
	Has exemption been granted for dedicated interface?						
Day	Uptime (%)	Downtime (%)	Response (millisecs)	PISP response (millisecs)	AISP response (millisecs)	CBPII response (millisecs)	Error response rate (%)
	D	E	F	G	H	I	J
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							
26							
27							
28							
29							
30							
31							
32							
33							
34							
35							
36							
37							
38							
39							
40							
41							
42							
43							
44							
45							
46							
47							
48							
49							
50							
51							
52							
53							
54							
55							
56							
57							
58							
59							
60							
61							
62							
63							
64							
65							
66							
67							
68							
69							
70							
71							
72							
73							
74							
75							
76							
77							
78							
79							
80							
81							
82							
83							
84							
85							
86							
87							
88							
89							
90							
91							
92							

16 Annex 46BG Notes on completing REP020 Statistics on the availability and performance of a dedicated interface

These notes contain guidance for quarterly reporting by Account Servicing Payment Service Providers (ASPSPs) with payment accounts accessible online that are required to publish on their website quarterly statistics on the availability and performance of the dedicated interface and of the interface used by its payment service users under article 32(4) *EBA* Regulator Technical Standards on Strong Customer Authentication and Common and Secure Communication ("the *SCA-RTS*").

The following completion notes should be read in conjunction with *EBA* Guidelines on the conditions to benefit from an exemption from the contingency mechanism under article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC) ("the EBA Guidelines").

The form provides the means for ASPSPs to provide the *FCA* with quarterly statistics on the availability and performance of the dedicated interface and of the interface used by its *payment service users*.

'Account Servicing Payment Services Providers' has the same definition as at Regulation 2(1) Payment Services Regulations 2017.

All ASPSPs with payment accounts accessible online and providing access to account information service providers (AISPs), payment initiation service providers (PISPs), or card based payment instrument issuers (CBPIIs), via a 'dedicated interface' are required to provide data.

ASPSPs with payment accounts accessible online and providing access to AISPs, PISPs, or CBPIIs via means other than the dedicated interface are not required to report daily statistics on the availability and performance of such interfaces, and should submit a 'nil return'.

Structure of the return

REP020 requires the ASPSP to report daily statistics on the availability and performance for each of its payment service user interfaces and dedicated interfaces for the previous quarter, for the daily statistics published on the ASPSPs website in accordance with article 32(4) of the *SCA-RTS*.

For each dedicated interface, the ASPSP should indicate by selecting 'yes' or 'no' if the dedicated interface benefits from an exemption under article 33(6) of the *SCA-RTS*. This will be 'no' for any payment service user interface.

Availability

Availability of each dedicated interface and payment service user interface should be reported as a percentage of uptime (Column D) and downtime (Column E).

To calculate the availability of each interface, the ASPSP should:

- calculate the percentage uptime as 100% minus the percentage downtime;
- calculate the percentage downtime using the total number of seconds the dedicated interface was down in a 24-hour period starting and ending at midnight;

- count the interface as 'down' when five consecutive requests for access to information for the provision of payment initiation services, account information services or confirmation of availability of funds are not replied to within a total timeframe of 30 seconds, irrespective of whether these requests originate from one or multiple PISPs, AISPs or CBPIIs. In such case, the ASPSP should calculate downtime from the moment it has received the first request in the series of five consecutive requests that were not replied to within 30 seconds, provided that there is no successful request in between those five requests to which a reply has been provided.

Performance

Performance should be reported for each interface based on the daily average time in milliseconds.

At column F, ASPSPs should report daily statistics for each payment service user interface on the daily average time (in milliseconds) taken, per request, for the ASPSP to respond to payment service user requests in that interface.

At column G, ASPSPs should report daily statistics for each dedicated interface on the daily average time (in milliseconds) taken, per request, for the ASPSP to provide to the account information service provider (AISP) all the information requested in accordance with article 66(4)(b) of PSD2 and Article 36(1)(b) of the *SCA-RTS*.

At column H, ASPSPs should report daily statistics for each dedicated interface on the daily average time (in milliseconds) taken, per request, for the ASPSP to provide to the payment initiation service provider (PISP) all the information requested in accordance with article 36(1)(a) of the *SCA-RTS*.

At column I, ASPSPs should report daily statistics for each dedicated interface on the daily average time (in milliseconds) taken, per request, for the ASPSP to provide to the card based payment instrument issuer (CBPII) or to the PISP a 'yes/no' confirmation in accordance with article 65(3) of PSD2 and article 36(1)(c) of the *SCA-RTS*.

At column J, ASPSPs should report daily statistics for each dedicated interface on the daily error response rate as a percentage – calculated as the number of error messages concerning errors attributable to the ASPSP sent by the ASPSP to the PISPs, AISPs and CBPIIs in accordance with article 36(2) of the *SCA-RTS* per day, divided by the number of requests received by the ASPSP from AISPs, PISPs and CBPIIs in the same day and multiplied by 100.

Data elements

Quarterly statistics on availability and performance of dedicated interfaces	
1A – Do you wish to make a nil return?	ASPSPs providing payment accounts accessible online and facilitating access to AISPs, PISPs or CBPIIs via a dedicated interface must submit a return each quarter and should select 'no'. ASPSPs providing access via other means other than a dedicated interface are not required to submit a return and should select 'yes'.
2A – Interface Name/Id	ASPSPs submitting a return should provide the name or ID used within the PSP to identify the interface being reported on. This should indicate whether the interface is a dedicated interface or a payment service user

	interface. Where relevant, it should be the same ID used when the ASPSP submitted a request for exemption from the contingency mechanism (max 100 characters).
Availability statistics	
2B – Interface type	Select what type of interface the statistics are being provided for: • PSU interface • Dedicated interface
2C – Has exemption been granted for dedicated interface?	Select 'yes' or 'no' indicating if the interface has been exempted under article 33(6) of the *SCA RTS*.
2D – Uptime (%)	ASPSPs should report the uptime of the interface as a percentage in accordance with the calculation method at GL 2.4(a) *EBA* Guidelines for each day in the reporting period (up to 92 days where applicable). Percentage figure should be provided to two decimal places.
2E – Downtime (%)	ASPSPs should report the downtime of the interface as a percentage in accordance with the calculation method at GL 2.4(b) *EBA* Guidelines for each day in the reporting period (up to 92 days where applicable). Percentage figure should be provided to two decimal places.
Performance statistics	
Payment Services User (PSU) interface	
2F – response (millisecs)	Only to be completed if "PSU interface" has been selected at 2B. ASPSPs should provide the daily average response time, (in milliseconds expressed as a whole number, e.g. 1.5 seconds is represented as 1500 milliseconds) taken per request, for the ASPSP to respond to requests from payment service user via the payment service user interface.
Dedicated interface	
2G – AISP response (millisecs)	Only to be completed if "Dedicated interface" has been selected at 2B. ASPSPs should provide the daily average time (in milliseconds expressed as a whole number, e.g. 1.5 seconds is represented as 1500 milliseconds) taken, per request, for the ASPSP to provide to the account information service provider (AISP) all the information requested in accordance with article 66(4)(b) of PSD2 and article 36(1)(b) of the *SCA RTS*.
2H – PISP response (millisecs)	Only to be completed if "Dedicated interface" has been selected at 2B. ASPSPs should provide the daily average time (in milliseconds expressed as a whole number, e.g. 1.5 seconds is represented as 1500 milliseconds) taken, per request, for the ASPSP to provide to the payment initiation service provider (PISP) all the information requested in accordance with article 36(1)(a) of the *SCA RTS*.
2I – CBPII response (millisecs)	Only to be completed if "Dedicated interface" has been selected at 2B. ASPSPs should provide the daily average time (in milliseconds expressed as a whole number, e.g. 1.5 seconds is represented as 1500 milliseconds) taken, per request, for the ASPSP to provide to the card based payment instrument issuer (CBPII) or to the PISP a 'yes/no' confirmation in accordance with article 65(3) of PSD2 and article 36(1)(c) of the RTS.

2J – Error response rate	Only to be completed if "Dedicated interface" has been selected at 2B. ASPSPs should provide the daily error response rate – calculated as the number of error messages concerning errors attributable to the ASPSP sent by the ASPSP to the PISPs, AISPs and CBPIIs in accordance with article 36(2) of the RTS per day, divided by the number of requests received by the ASPSP from AISPs, PISPs and CBPIIs in the same day. Percentage figure should be provided to two decimal places.

Annex C

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 D

Amendments to the Dispute Resolution: Complaints sourcebook (DISP)

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

1 Treating complainants fairly

…

1 Annex 1ADR 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 1AAG 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').

…

TP 1 Transitional provisions

1.1 Transitional provisions table

(1)	(2) Material provision to which transitional provision applies	(3)	(4) Transitional provision	(5) Transitional provision: dates in force	(6) Handbook provision: coming into force
…					
53	*DISP* 1 Annex 1AD	R	The figures for complaints relating to alleged *authorised push payment fraud* in Table 4 should only include such complaints from 1 July 2019.	1 July 2019 to 30 June 2020	1 July 2019

Annex E

Amendments to the Credit Unions sourcebook (CREDS)

In this Annex, underlining indicates new text.

9 Annex 1R **Credit union complaints return**

…

Credit-related complaints Section 5A

…

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

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

…

Notes on completion of this return

…

Section 5A – Credit-related complaints

…

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').

…

…

TP 1 **Transitional Provision**

(1)	(2) Material provision to which transitional provision applies	(3)	(4) Transitional provision	(5) Transitional provision: dates in force	(6) Handbook provision: coming into force
…					
19	*CREDS* 9 Annex 1	R	The figures for complaints relating to alleged *authorised push payment fraud* in Section 5B should only include such complaints from 1 July 2019.	1 July 2019 to 31 March 2020	1 July 2019

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

…

15.2 General

Q9. If we provide payment services to our clients, will we always require authorisation or registration under the regulations?

Not necessarily; you will only be providing payment services, for the purpose of the regulations, when you carry on one or more of the activities in *PERG* 15 Annex 2:

as a regular occupation or business activity; and

these are not excluded or exempt activities (see *PERG* 15.5 Negative scope/exclusions).

…

15.3 Payment services

…

Q25A. When might we be providing an account information service?

…

Whether a service is an account information service depends on whether there has been access to payment accounts. The account information service provider is subject to rights and obligations concerning such access under the PSRs 2017 (see Chapter 17 of the Approach Document). For a service to be an account information service it is also necessary for it to involve the provision of payment account information to the payment service user that has been consolidated in some way (although a service may be an account information service even if the information relates to only one payment account).

In our view, an account information service is not provided if the only information provided to the customer is the customer's name, account number and sort code.

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.

A business that obtains and processes payment account information in support of an authorised or registered account information service provider, but does not itself provide the information to the user, is a technical service provider. It does not require authorisation or registration as an account information service provider. The authorised or registered account information service provider is responsible for compliance with the PSRs 2017 where account access is outsourced to a technical service provider.

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 must be between the customer and Firm A, the principal.

…

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 must 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.

Q40. 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 [deleted]

~~Q47. 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.~~