PAYMENT SERVICES (AMENDMENT No 2) INSTRUMENT 2020

Powers exercised

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

(1) the following regulations of the Payment Services Regulations 2017:

(a) Regulation 98(3) (Management of operational and security risks);
(b) Regulation 109 (Reporting requirements); and
(c) Regulation 120 (Guidance); and

(2) Regulation 3 (Delegation) of the Financial Regulators' Powers (Technical Standards etc.) (Amendment etc.) (EU Exit) Regulations 2018 ("the Regulations").

Pre-conditions to making

B. The FCA has consulted the Prudential Regulation Authority and the Bank of England as appropriate in accordance with regulation 5 of the Regulations.

C. A draft of this instrument has been approved by the Treasury, the Minister considering that it makes appropriate provision to prevent, remedy or mitigate any failure of retained EU law to operate effectively, or any other deficiency in retained EU law, arising from the withdrawal of the United Kingdom from the European Union.

Commencement

D. This instrument comes into force on IP completion day as defined in the European Union (Withdrawal Agreement) Act 2020, at exactly the same time as the Technical Standards on Strong Customer Authentication and Common and Secure Methods of Communication Instrument 2020 comes into force.

[**Note:** IP completion day is 11pm on 31 December 2020.]

Amendments to the Handbook

E. The Glossary of definitions is amended in accordance with Annex A to this instrument.

F. The Supervision manual (SUP) is amended in accordance with Annex B to this instrument.

Notes

G. 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

H. This instrument may be cited as the Payment Services (Amendment No 2) Instrument 2020.

By order of the Board
26 November 2020

Annex A

Amendment to the Glossary of definitions

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

Amend the following definition as shown.

SCA RTS	~~Regulation (EU) 2018/389 (RTS)~~ technical standards on strong customer authentication and common and secure ~~open standards~~ methods of communication made by the *FCA* under Regulation 106A of the *Payment Services Regulations*.

Annex B

Amendments to the Supervision manual (SUP)

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

…

15C Applications under the Payment Services Regulations

…

15C.2 Request for exemption from the obligation to set up a contingency mechanism (Article 33(6) of the SCA RTS)

…

15C.2.3 G The *EBA* issued the Guidelines ~~on 4 December 2018~~ on the conditions to ~~be met to~~ benefit from an exemption from the contingency ~~measures~~ mechanism under article 33(6) of ~~the *SCA RTS*~~ Regulation (EU) 2018/389 (RTS on SCA and CSC) (EBA/GL/2018/07) on the 4 December 2018. 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.2.5 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 the contingency ~~measures~~ mechanism under article 33(6) of the *SCA RTS*.

15C Annex 1D Form: Request for exemption from the obligation to set up a contingency mechanism

…

ASPSPs completing the form should also ~~comply with~~ apply the Guidelines on the conditions ~~to be met~~ to benefit from an exemption from the contingency ~~measures~~

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

		Column A	Column B	Column C
Article	**Requirement**	**…**	**Summary of how the implementation of these specifications fulfils the requirements of ~~PSD2~~ the *Payment Services Regulations*, *SCA-RTS* and FCA Guidelines** **…**	**…**
~~PSD2 Article 67~~ Regulation 70 *Payment Services Regulations* ~~SCA-RTS~~ *SCA RTS* Article 30 ~~RTS~~	Enabling AISPs to access the necessary data from payment accounts accessible online			
~~PSD2 Article 65 & 66~~ Regulations 68 and 69 *Payment Services Regulations* ~~SCA-RTS~~ *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~~ *SCA RTS* Article 30(3)	Conforming to (widely used) standard(s) of communication issued by international or European standardisation organisations			
~~PSD2 Article 64(2)~~ Regulation 67(2) *Payment Services Regulations* ~~SCA-RTS~~ *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)~~ Regulations 69(3)(b) and 70(3)(b) of the *Payment Services Regulations*	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)~~ Regulations 68(3)(c), 69(3)(d) and 70(3)(c) *Payment Services Regulations* ~~SCA-RTS~~ *SCA RTS* Article 30(1)(a) and 34	Enabling the identification of the AISP/PISP/CBPII and support eIDAS for certificates			
~~SCA RTS~~ *SCA RTS* Article 10(2)(b)	Allowing for no more than 90 days re-authentication for AISPs			
~~SCA RTS~~ *SCA RTS* Article 36(5)	Enabling the ASPSPs and			

	AISPs to count the number of access requests during a given period			
~~SCA-RTS~~ *SCA RTS* Article 30(4)	Allowing for a change control process			
~~PSD2 Article 64(2) and 80(2) and 80(4)~~ Regulations 67(2), 83(2) and 83(4) *Payment Services Regulations*	Allowing for the possibility for an initiated transaction to be cancelled in accordance with ~~PSD2~~ the *Payment Services Regulations*, including recurring transactions			
~~SCA-RTS~~ *SCA RTS* Article 36(2)	Allowing for error messages explaining the reason for the unexpected event or error			
~~PSD2 Article 19(6)~~ Regulation 25(1) *Payment Services Regulations*	Supporting access via technology service providers on behalf of authorised actors			
~~PSD2 Article 97(5)~~ Regulation 100(4) *Payment Services Regulations* and ~~SCA-RTS~~ *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)~~ Regulation 70(3)(d) *Payment Services Regulations* ~~and 30(1)(b) and~~	Enabling the AISP to access the same information as accessible to the payment servicer user in relation to			

~~SCA RTS~~ *SCA RTS* Article 36(1)(a) and 30(1)(b)	their designated payment accounts and associated payment transactions			
~~SCA RTS~~ *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)~~ Regulation 100(2) *Payment Services Regulations* and ~~SCA RTS~~ *SCA RTS* Article 5	Enabling the dynamic linking to a specific amount and payee, including batch payments			
~~SCA RTS~~ *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~~ *SCA RTS* Article 4	Enabling strong customer authentication composed of two different elements			
~~SCA RTS~~ *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)~~ Regulation 100(3) *Payment Services Regulations* ~~SCA-RTS~~ *SCA RTS* Articles 30(2)(c) and 35	Ensuring security at transport and application level			
~~PSD2 Article 97(3)~~ Regulation 100(3) *Payment Services Regulations* ~~SCA-RTS~~ *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~~ *SCA RTS* Article 29	Allowing for traceability			
~~SCA-RTS~~ *SCA RTS* Article 32	Allowing for the ASPSP's dedicated interface to provide at least the same availability and performance as the user interface			

…

…

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			
…				
	Notification that the reference fraud rate is exceeded			
…				
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~~ GBP 440		
		~~EUR 250~~ GBP 220		
		~~EUR 100~~ GBP 85		
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~~ GBP 440		
		~~EUR 250~~ GBP 220		
		~~EUR 100~~ GBP 85		

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~~ GBP 440		
		~~EUR 250~~ GBP 220		
		~~EUR 100~~ GBP 85		
…				
	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~~ GBP 440		
		~~EUR 250~~ GBP 220		
		~~EUR 100~~ GBP 85		
…				

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 problem with the dedicated interface	
…		
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~~ *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~~ *SCA RTS* article 32(3) and the 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 and CSC) published on 4 December 2018 (EBA/GL/2018/07) and Opinion on the implementation of the RTS on SCA and CSC (EBA-2018-Op-04)). [ ] Other failure to comply with article 32.

…		

16 Reporting requirements

…

16.13 Reporting under the Payment Services Regulations

…

16.13.8A G ~~*Payment service providers* should use the~~ The return in *SUP* 16 Annex 27ED ~~to comply with~~ reflects the *EBA*'s Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2), published on 18 July 2018 (EBA/GL/2018/05). ~~*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~~

…

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*~~ *Payment Services Regulations*.

16.13.19 D …

(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*~~ *Payment Services Regulations*.

…

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~~,~~ and SUP 16.13.7D ~~and~~. The notes also build

on the EBA Guidelines on fraud reporting under the ~~Second~~ Payment Services Directive 2 (PSD2) (EBA/GL/2018/05) ("the EBA Guidelines").

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

…

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.~~

…

Table 1 - What is a fraudulent transaction?

…

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~~ the provisions in the *Payment Services Regulations*.

…

Data elements

<table>
<tr><td colspan="2">Table 1 – Payment transactions and fraudulent payment transactions for payment services
Value should be reported in pounds sterling throughout (£)</td></tr>
<tr><td colspan="2">…</td></tr>
<tr><td>2A-2L
38A–38L
48A–48L
103A–103L
155A–155L
167A–167L
199A–199L
200A–200L</td><td>• 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;</td></tr>
</table>

	• 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. **PSPs should continue to report fraud data broken down into domestic, cross border within the EEA, and cross border outside the EEA as set out in Columns A-F, notwithstanding the UK's withdrawal from the EU.**
…	
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)~~.
…	
Remote transactions	
6A-6L (credit transfers) 51A–51L (card payments)	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.

106A–106L (card payments acquired) 168A–168L (e-money payment 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))~~ (Regulation 2 of the *Payment Services Regulations*).
…	
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 *Payment Services Regulations*, the final fraud loss figures should not take into account such refunds.
…	

…

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*")~~ *SCA RTS*.

…

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~~ regulation 69(2)(b) of the *Payment Services Regulations* and ~~Article~~ article 36(1)(b) of the ~~*SCA-RTS*~~ *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*~~ *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~~ regulation 68(4), (7) and (8) of the *Payment Services Regulations* and article 36(1)(c) of the ~~*SCA-RTS*~~ *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*~~ *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	
…	
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~~ Regulation 69(2)(b) of the *Payment Services Regulations* 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 /PISP yes/no 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~~ regulation 68(4), (7) and (8) of the *Payment Services Regulations* and article 36(1)(c) of the ~~RTS~~ *SCA 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~~ *SCA 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.