PAYMENT SERVICES INSTRUMENT 2018

Powers exercised

A. The Financial Conduct Authority makes this instrument in the exercise of the following powers and related provisions in the Payment Services Regulations 2017 (SI 2017/52) ("the Regulations"):

(1) regulation 98 (Management of operational and security risk);
(2) regulation 109 (Reporting requirements); and
(3) regulation 120 (Guidance).

Commencement

B. This instrument comes into force on 29 June 2018.

Amendments to the Handbook

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

Notes

D. 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

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

By order of the Board
28 June 2018

Annex

Amendments to the Supervision manual (SUP)

Insert the following new text after SUP 16.13.8G.

Operational and Security Risk assessments

16.13.9 G Regulation 98(1) of the *Payment Services Regulations* provides that each *payment service provider* must establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks relating to the *payment services* it provides.

16.13.10 G Regulation 98(2) of the *Payment Services Regulations* provides that each *payment service provider* must provide to the *FCA* an updated and comprehensive assessment:

(1) of the operational and security risks relating to the *payment services* it provides; and

(2) on the adequacy of the mitigation measures and control mechanisms implemented in response to those risks.

The purpose of *SUP* 16.13.11G to 16.13.17G is to direct the form and manner of the assessment and the information that the assessment must contain.

16.13.11 G The *EBA* issued Guidelines on 12 December 2017 on the security measures for operational and security risks of payment services under the *Payment Services Directive*. The Guidelines specify requirements for the establishment, implementation and monitoring of the security measures that *payment service providers* must take to manage operational and security risks relating to the *payment services* they provide.

[**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]

16.13.12 D *Payment service providers* must comply with the *EBA's* Guidelines on security measures for operational and security risks of payment services as issued on 12 December 2017 where they are addressed to *payment service providers.*

16.13.13 D The assessments required by regulation 98(2) of the *Payment Services Regulations* must be submitted to the *FCA*:

(1) at least once every calendar year;

(2) in writing, in the form specified in *SUP* 16 Annex 27GD, and attaching the documents described in that form; and

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

16.13.14 G *Payment service providers* should submit the form and the assessments to the *FCA* in accordance with *SUP* 16.13.13D(2) as soon as practicable after the assessments have been completed.

16.13.15 G *Payment service providers* may provide operational and security risk assessments to the *FCA* on a more frequent basis than once every calendar year if they so wish. *Payment service providers* should not, however, submit such assessments more frequently than once every quarter.

16.13.16 G Subject to the requirements in *SUP* 16.13.13D, *payment service providers* should submit a nil return for each quarter in which they do not make a submission to the *FCA*.

16.13.17 G *Payment service providers* should note that article 16(3) of Regulation (EU) No. 1093/2010 also requires them to make every effort to comply with the *EBA*'s Guidelines on security measures for operational and security risks of payment services.

After SUP 16 Annex 27F (Notes on completing REP017 Payments Fraud Report) insert the following new Annexes as SUP 16 Annex 27G and SUP 16 Annex 27H.

16 Annex 27GD **REP018 Operational and Security Risk reporting form**

This form can be found at the following address:
https://www.handbook.fca.org.uk/form/sup/SUP_16_ann_27G_REP018_20180629.pdf

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.	

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

Operational and security risk form

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.

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]