Incident reporting – Amendments to Payment Services and Electronic Money – Our Approach

18 March 2026

Introduction

This document sets out amendments to the Payment Services and Electronic Money – Our Approach document following publication of new incident reporting rules and guidance in PS26/2 and FG26/3. The rules apply from 18 March 2027.

Amendments

3.80 API Guideline 9 and EMI Guideline 9 explain the information and documentation required with respect to procedures for monitoring, handling and following up security incidents and security-related customer complaints. The information required should include details of how the applicant will comply with its obligation to report major operational or security incidents under regulation 99 of the PSRs 2017 – **see Chapter 13 – Reporting and notifications** and SUP 15.14 and 15.18 for more information on the incident reporting r~~R~~equirements ~~andEBA Guidelines on major incident reporting~~.[1]

4.18 An EMI or PI should notify the Customer Contact Centre of any significant failure in its systems or controls, including those reported to the EMI or PI by its auditor (if applicable). Reporting requirements covered by regulation 99 of the PSRs 2017 may also apply. ~~(and the European Banking Authority Guidelines on major incidents reporting under the Revised Payment Services Directive is relevant to those).~~

8.50 Credit institutions are defined as operators of essential services under NIS Regulations, in so far as they meet the criteria set out in Article 8 of NIS. ~~The EBA's guidelines on Major Incident Reporting confirm that the requirements for notification of incidents under PSD2 are considered to be at least equivalent to the obligations in the European Directive (EU) 2016/1148 which the NIS Regulations originally implemented.~~ Incidents affecting a credit institution's payment services should be reported under ~~PSD2~~ the PSRs 2017 rather than NIS.

13.12 **Notification required – Notification of major operational or security incidents – ~~PSD2~~ PSRs 2017**

Required to notify: All PSPs are required to notify us without undue delay if they become aware of a major operational or security incident. ~~SUP 15.14.20 D requires PSPs to comply with the EBA Guidelines on major incident reporting under PSD2. These Guidelines specify~~ According to SUP 15.14.18BG, a PSP should use the thresholds specified in SUP 15.18.6R(1) to assess whether an operational or security incident is

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

major and needs to be reported to us. SUP15.14.18CD requires PSPs to comply with the relevant requirements applicable to enhanced reporting firms in SUP 15.18 when submitting the report, including the format for the report and the procedures the PSP should follow. Our finalised guidance FG26/3 sets out case studies with examples of some of the types of incidents we would expect a PSP to report under the PSRs 2017 and SUP 15.18. ~~These Guidelines also specify the format for the notification and the procedures the PSP should follow. PSPs are required to submit an initial, intermediate and final notification.~~

When to notify: The notification channel is usually available at all times.

The initial phase of the report ~~notification should be~~ must be submitted to us within the first 4 hours from the moment the incident was detected, or, if the notification channel is not available or operational at that time, as soon as it becomes available or operational again. ~~We may direct PSPs to submit initial notifications at times other than those specified above.~~ For the intermediate phase of the report, a PSP must submit the additional information ~~An intermediate report should be submitted, using the same method~~, as soon as is practicable after any significant change in circumstances from those described in the report ~~every time there is a relevant status update to the incident As a minimum, it should be submitted by the date indicated in the previous report (either the initial report or the previous intermediate report)~~. If there is any further significant change in circumstances from those described in the previous submission by the PSP (including the incident being resolved), the PSP must as soon as is practicable after such change submit this information to the FCA. ~~A final report~~ For the final phase of the report, the PSP must submit the additional information ~~be submitted when the root cause analysis has taken place (regardless of whether mitigation measures have already been implemented or the final root cause has been identified) and there are actual figures available to replace any earlier estimates~~. This must be within 30 working days, or where this is impracticable, as soon as is practicable but in any event within 60 working days of the incident being resolved.

Method of submission: Connect

Handbook references: ~~SUP 15.14.16~~ SUP 15.14.18G ~~to 15.14.22~~ 15.14.23G, SUP 15.18 and ~~SUP 15 Annex 11D~~ SUP 15 Annex 1R, GEN 2.2.36(9)-(13)

Content and purpose

This notification is required under Regulation 99 of the PSRs 2017. The notification must include the information set out ~~in the template form cited in~~ in ~~SUP 15 Annex 11D~~ SUP 15 Annex1R and must be in writing.

Requiring PSPs to notify us of major operational or security incidents helps us discharge our supervisory functions by providing us with information on the most serious operational and security incidents.

Process

Businesses should follow the instructions on Connect to submit their notifications electronically

17.177 Problems with dedicated interfaces should also be separately assessed against the thresholds in SUP 15.18.6R(1) ~~the EBA Guidelines~~ to determine whether they qualify as a major incident in accordance with SUP 15.14.18BG (see Chapter 13 – Reporting and notifications)