EBA/GL/2017/10

19/12/2017

Guidelines

on major incident reporting under Directive (EU) 2015/2366 (PSD2)

1. Compliance and reporting obligations

Status of these Guidelines

1. This document contains Guidelines issued pursuant to Article 16 of Regulation (EU) No 1093/2010.[1] In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authorities and financial institutions must make every effort to comply with the Guidelines.

2. Guidelines set out the EBA's view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. Competent authorities as defined in Article 4(2) of Regulation (EU) No 1093/2010 to whom Guidelines apply should comply by incorporating them into their practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where Guidelines are directed primarily at institutions.

Reporting requirements

3. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authorities must notify the EBA that they comply or intend to comply with these Guidelines, or otherwise give reasons for non-compliance, by 19.02.2018. In the absence of any notification by this deadline, competent authorities will be considered by the EBA to be non-compliant. Notifications should be sent by submitting the form available on the EBA website to compliance@eba.europa.eu with the reference 'EBA/GL/2017/10'. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities. Any change in the status of compliance must also be reported to the EBA.

4. Notifications will be published on the EBA website, in line with Article 16(3).

[1] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12).

2. Subject matter, scope and definitions

Subject matter

5. These Guidelines derive from the mandate given to the EBA in Article 96(3) of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (PSD2).

6. In particular, these Guidelines specify the criteria for the classification of major operational or security incidents by payment service providers as well as the format and procedures they should follow to communicate, as laid down in Article 96(1) of the above-mentioned directive, such incidents to the competent authority in the home Member State.

7. In addition, these Guidelines deal with the way these competent authorities should assess the relevance of the incident and the details of the incident reports that, according to Article 96(2) of the said directive, they shall share with other domestic authorities.

8. Moreover these Guidelines also deal with the sharing with the EBA and the ECB of the relevant details of the incidents reported, for the purposes of promoting a common and consistent approach.

Scope of application

9. These Guidelines apply in relation to the classification and reporting of major operational or security incidents in accordance with Article 96 of Directive (EU) 2015/2366.

10. These Guidelines apply to all incidents included under the definition of 'major operational or security incident', which covers both external and internal events that could be either malicious or accidental.

11. These Guidelines apply also where the major operational or security incident originates outside the Union (e.g. when an incident originates in the parent company or in a subsidiary established outside the Union) and affects the payment services provided by a payment service provider located in the Union either directly (a payment-related service is carried out by the affected non-Union company) or indirectly (the capacity of the payment service provider to keep carrying out its payment activity is jeopardised in some other way as a result of the incident).

Addressees

12. The first set of Guidelines (Section 4) is addressed to payment service providers as defined in Article 4(11) of Directive (EU) 2015/2366 and as referred to in Article 4(1) of Regulation (EU) 1093/2010.

13. The second and third sets of Guidelines (Sections 5 and 6) are addressed to competent authorities as defined in Article 4(2)(i) of Regulation (EU) No 1093/2010.

Definitions

14. Unless otherwise specified, terms used and defined in the Directive (EU) 2015/2366 have the same meaning in the Guidelines. In addition, for the purposes of these Guidelines, the following definitions apply:

Operational or security incident	A singular event or a series of linked events unplanned by the payment service provider which has or will probably have an adverse impact on the integrity, availability, confidentiality, authenticity and/or continuity of payment-related services.
Integrity	The property of safeguarding the accuracy and completeness of assets (including data).
Availability	The property of payment-related services being accessible and usable by payment service users.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities or processes.
Authenticity	The property of a source being what it claims to be.
Continuity	The property of an organisation's processes, tasks and assets needed for the delivery of payment-related services being fully accessible and running at acceptable predefined levels.
Payment-related services	Any business activity in the meaning of Article 4(3) of PSD2, and all the necessary technical supporting tasks for the correct provision of payment services.

3. Implementation

Date of application

15. These Guidelines apply from 13 January 2018.

4. Guidelines addressed to payment service providers on the notification of major operational or security incidents to the competent authority in their home Member State

Guideline 1: Classification as major incident

1.1. Payment service providers should classify as major those operational or security incidents that fulfil

a. one or more criteria at the 'Higher impact level', or

b. three or more criteria at the 'Lower impact level'

as set out in GL 1.4, and following the assessment set out in these Guidelines.

1.2. Payment service providers should assess an operational or security incident against the following criteria and their underlying indicators:

i. Transactions affected

Payment service providers should determine the total value of the transactions affected, as well as the number of payments compromised as a percentage of the regular level of payment transactions carried out with the affected payment services.

ii. Payment service users affected

Payment service providers should determine the number of payment service users affected both in absolute terms and as a percentage of the total number of payment service users.

iii. Service downtime

Payment service providers should determine the period of time when the service will probably be unavailable for the payment service user or when the payment order, in the meaning of Article 4(13) of PSD2, cannot be fulfilled by the payment service provider.

iv. Economic impact

Payment service providers should determine the monetary costs associated with the incident holistically and take into account both the absolute figure and, when applicable, the relative importance of these costs in relation to the size of the payment service provider (i.e. to the payment service provider's Tier 1 capital).

v. High level of internal escalation

Payment service providers should determine whether or not this incident has been or will probably be reported to their executive officers.

vi. Other payment service providers or relevant infrastructures potentially affected

Payment service providers should determine the systemic implications that the incident will probably have, i.e. its potential to spill over beyond the initially affected payment service provider to other payment service providers, financial market infrastructures and/or card payment schemes.

vii. Reputational impact

Payment service providers should determine how the incident can undermine users' trust in the payment service provider itself and, more generally, in the underlying service or the market as a whole.

1.3. Payment service providers should calculate the value of the indicators according to the following methodology:

i. Transactions affected

As a general rule, payment service providers should understand as 'transactions affected' all domestic and cross-border transactions that have been or will probably be directly or indirectly affected by the incident and, in particular, those transactions that could not be initiated or processed, those for which the content of the payment message was altered and those that were fraudulently ordered (whether the funds have been recovered or not).

Furthermore, payment service providers should understand the regular level of payment transactions to be the daily annual average of domestic and cross-border payment transactions carried out with the same payment services that have been affected by the incident, taking the previous year as the reference period for calculations. If payment service providers do not consider this figure to be representative (e.g. because of seasonality), they should use another, more representative, metric instead and convey to the competent authority the underlying rationale for this approach in the corresponding field of the template (see Annex 1).

ii. Payment service users affected

Payment service providers should understand as 'payment service users affected' all customers (either domestic or from abroad, consumers or corporates) that have a contract with the affected payment service provider that grants them access to the affected payment service, and that have suffered or will probably suffer the consequences of the incident. Payment service providers should resort to estimations based on past activity to determine the number of payment service users that may have been using the payment service during the lifetime of the incident.

In the case of groups, each payment service provider should consider only its own payment service users. In the case of a payment service provider offering operational services to others, that payment service provider should consider only its own payment service users

(if any), and the payment service providers receiving those operational services should assess the incident in relation to their own payment service users.

Furthermore, payment service providers should take as the total number of payment service users the aggregated figure of domestic and cross-border payment service users contractually bound to them at the time of the incident (or, alternatively, the most recent figure available) and with access to the affected payment service, regardless of their size or whether they are considered active or passive payment service users.

iii. Service downtime

Payment service providers should consider the period of time that any task, process or channel related to the provision of payment services is or will probably be down and, thus, prevents (i) the initiation and/or execution of a payment service and/or (ii) access to a payment account. Payment service providers should count the service downtime from the moment the downtime starts, and they should consider both the time intervals when they are open for business as required for the execution of payment services as well as the closing hours and maintenance periods, where relevant and applicable. If payment service providers are unable to determine when the service downtime started, they should exceptionally count the service downtime from the moment the downtime is detected.

iv. Economic impact

Payment service providers should consider both the costs that can be connected to the incident directly and those which are indirectly related to the incident. Among other things, payment service providers should take into account expropriated funds or assets, replacement costs of hardware or software, other forensic or remediation costs, fees due to non-compliance with contractual obligations, sanctions, external liabilities and lost revenues. As regards the indirect costs, payment service providers should consider only those that are already known or very likely to materialise.

v. *High level of internal escalation*

Payment service providers should consider whether or not, as a result of its impact on payment-related services, the Chief Information Officer (or similar position) has been or will probably be informed about the incident outside any periodical notification procedure and on a continuous basis throughout the lifetime of the incident. Furthermore, payment service providers should consider whether or not, as a result of the impact of the incident on payment-related services, a crisis mode has been or is likely to be triggered.

vi. *Other payment service providers or relevant infrastructures potentially affected*

Payment service providers should assess the impact of the incident on the financial market, understood as the financial market infrastructures and/or card payment schemes that support them and other payment service providers. In particular, payment service providers should assess whether or not the incident has been or will probably be replicated at other payment service providers, whether or not it has affected or will probably affect the smooth functioning of financial market infrastructures and whether or not it has compromised or will probably compromise the sound operation of the financial system as a

whole. Payment service providers should bear in mind various dimensions such as whether the component/software affected is proprietary or generally available, whether the compromised network is internal or external and whether or not the payment service provider has stopped or will probably stop fulfilling its obligations in the financial market infrastructures of which it is a member.

vii. *Reputational impact*

Payment service providers should consider the level of visibility that, to the best of their knowledge, the incident has gained or will probably gain in the marketplace. In particular, payment service providers should consider the likelihood that the incident will cause harm to society as a good indicator of its potential to affect their reputation. Payment service providers should take into account whether or not (i) the incident has affected a visible process and is therefore likely to receive or has already received media coverage (considering not only traditional media, such as newspapers, but also blogs, social networks, etc.), (ii) regulatory obligations have been or will probably be missed, (iii) sanctions have been or will probably be breached or (iv) the same type of incident has occurred before.

1.4. Payment service providers should assess an incident by determining, for each individual criterion, if the relevant thresholds in Table 1 are or will probably be reached before the incident is resolved.

Table 1: Thresholds

Criteria	Lower impact level	Higher impact level
Transactions affected	> 10% of the payment service provider's regular level of transactions (in terms of number of transactions) **and** > EUR 100 000	> 25% of the payment service provider's regular level of transactions (in terms of number of transactions) **or** > EUR 5 million
Payment service users affected	> 5 000 **and** > 10% of the payment service provider's payment service users	> 50 000 **or** > 25% of the payment service provider's payment service users
Service downtime	> 2 hours	Not applicable
Economic impact	Not applicable	> Max. (0.1% Tier 1 capital,* EUR 200 000) **or** > EUR 5 million
High level of internal escalation	Yes	Yes, and a crisis mode (or equivalent) is likely to be called upon
Other payment service providers or relevant infrastructures potentially affected	Yes	Not applicable
Reputational impact	Yes	Not applicable

*Tier 1 capital as defined in Article 25 of Regulation (EU) No 575/2013 of the European Parliament and of the Council, of 26 June 2013, on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012.

1.5. Payment service providers should resort to estimations if they do not have actual data to support their judgments of whether or not a given threshold is or will probably be reached before the incident is resolved (e.g. this could happen during the initial investigation phase).

1.6. Payment service providers should carry out this assessment on a continuous basis during the lifetime of the incident, to identify any possible status change, either upwards (from non-major to major) or downwards (from major to non-major).

Guideline 2: Notification process

2.1. Payment service providers should collect all relevant information, produce an incident report using the template provided in Annex 1 and submit it to the competent authority in the home Member State. Payment service providers should fill out the template following the instructions provided in Annex 1.

2.2. Payment service providers should use the same template to inform the competent authority throughout the lifetime of the incident (i.e. for initial, intermediate and final reports, as described in paragraphs 2.7 to 2.21). Payment service providers should complete the template in an incremental manner, on a best effort basis, as more information becomes readily available in the course of their internal investigations.

2.3. Payment service providers should also present to the competent authority in their home Member State, if applicable, a copy of the information provided (or that will be provided) to their users, as laid down in the second paragraph of Article 96(1) of PSD2, as soon as it is available.

2.4. Payment service providers should furnish the competent authority in the home Member State, if available and deemed relevant for the competent authority, with any additional information by appending supplementary documentation to the standardised template as one or various annexes.

2.5. Payment service providers should follow up on any requests from the competent authority in the home Member State to provide additional information or clarifications regarding already submitted documentation.

2.6. Payment service providers should at all times preserve the confidentiality and integrity of the information exchanged with the competent authority in their home Member State and also authenticate themselves properly towards the competent authority in their home Member State.

Initial report

2.7. Payment service providers should submit an initial report to the competent authority in the home Member State when a major operational or security incident is first detected.

2.8. Payment service providers should send the initial report to the competent authority within 4 hours from the moment the major operational or security incident was first detected, or, if the reporting channels of the competent authority are known not to be available or operational at that time, as soon as they become available/operational again.

2.9. Payment service providers should also submit an initial report to the competent authority in the home Member State when a previously non-major incident becomes a major incident. In this particular case, payment service providers should send the initial report to the competent authority immediately after the change of status is identified, or, if the reporting channels of the competent authority are known not to be available or operational at that time, as soon as they become available/operational again.

2.10. Payment service providers should include headline-level information (i.e. section A of the template) in their initial reports, thus featuring some basic characteristics of the incident and its expected consequences based on the information available immediately after it was detected or reclassified. Payment service providers should resort to estimations when actual data are not available. Payment service providers should also include in their initial report the date for the next update, which should be as soon as possible and under no circumstances go beyond 3 business days.

Intermediate report

2.11. Payment service providers should submit intermediate reports every time they consider that there is a relevant status update and, as a minimum, by the date for the next update indicated in the previous report (either the initial report or the previous intermediate report).

2.12. Payment service providers should submit to the competent authority a first intermediate report with a more detailed description of the incident and its consequences (section B of the template). Moreover, payment service providers should produce additional intermediate reports by updating the information already provided in sections A and B of the template at least, when they become aware of new relevant information or significant changes since the previous notification (e.g. whether the incident has escalated or decreased, new causes identified or actions taken to fix the problem). In any case, payment service providers should produce an intermediate report at the request of the competent authority in the home Member State.

2.13. As in the case of initial reports, when actual data are not available payment service providers should make use of estimations.

2.14. Furthermore, payment service providers should indicate in each report the date for the next update, which should be as soon as possible and under no circumstances go beyond 3 business days. Should the payment service provider not be able to comply with the estimated date for the next update, it should contact the competent authority in order to explain the reasons behind the delay, propose a new plausible submission deadline (no longer than 3 business days) and send a new intermediate report updating exclusively the information regarding the estimated date for the next update.

2.15. Payment service providers should send the last intermediate report when regular activities have been recovered and business is back to normal, informing the competent authority of this circumstance. Payment service providers should consider that business is back to normal when activity/operations are restored to the same level of service/conditions as defined by the payment service provider or laid out externally by a Service Level Agreement (SLA) in terms of processing times, capacity, security requirements, etc., and contingency measures are no longer in place.

2.16. Should business be back to normal before 4 hours have passed since the incident was detected, payment service providers should aim to submit both the initial and the last intermediate report simultaneously (i.e. filling out sections A and B of the template) by the 4-hour deadline.

Final report

2.17. Payment service providers should send a final report when the root cause analysis has taken place (regardless of whether or not mitigation measures have already been implemented or the final root cause has been identified) and there are actual figures available to replace any estimates.

2.18. Payment service providers should deliver the final report to the competent authority within a maximum of 2 weeks after business is deemed back to normal. Payment service providers needing an extension of this deadline (e.g. if there are no actual figures on the impact available yet) should contact the competent authority before it has lapsed and provide an adequate justification for the delay, as well as a new estimated date for the final report.

2.19. Should payment service providers be able to provide all the information required in the final report (i.e. section C of the template) within the 4-hour window since the incident was detected, they should aim to submit in their initial report the information related to initial, last intermediate and final reports.

2.20. Payment service providers should aim to include in their final reports full information, i.e. (i) actual figures on the impact instead of estimations (as well as any other update needed in sections A and B of the template) and (ii) section C of the template, which includes the root cause, if already known, and a summary of measures adopted or planned to be adopted to remove the problem and prevent its recurrence in the future.

2.21. Payment service providers should also send a final report when, as a result of the continuous assessment of the incident, they identify that an already reported incident no longer fulfils the criteria to be considered major and is not expected to fulfil them before the incident is resolved. In this case, payment service providers should send the final report as soon as this circumstance is detected and, in any case, by the estimated date for the next report. In this particular situation, instead of filling out section C of the template, payment service providers should tick the box 'incident reclassified as non-major' and explain the reasons justifying this downgrading.

Guideline 3: Delegated and consolidated reporting

3.1. Where permitted by the competent authority, payment service providers wishing to delegate reporting obligations under PSD2 to a third party should inform the competent authority in the home Member State and ensure the fulfilment of the following conditions:

a. The formal contract or, where applicable, existing internal arrangements within a group, underpinning the delegated reporting between the payment service provider and the third party unambiguously defines the allocation of responsibilities of all parties. In particular, it clearly states that, irrespective of the possible delegation of reporting obligations, the affected payment service provider remains fully responsible and accountable for the fulfilment of the requirements set out in Article 96 of PSD2 and for the content of the information provided to the competent authority in the home Member State.

b. The delegation complies with the requirements for the outsourcing of important operational functions as set out in

   i. Article 19(6) of PSD2 in relation to payment institutions and e-money institutions, applicable mutatis mutandis in accordance with Article 3 of Directive 2009/110/EC (EMD); or

   ii. the CEBS Guidelines on outsourcing in relation to credit institutions.

c. The information is submitted to the competent authority in the home Member State in advance and, in any case, following any deadlines and procedures established by the competent authority, where applicable.

d. The confidentiality of sensitive data and the quality, consistency, integrity and reliability of the information to be provided to the competent authority is properly ensured.

3.2. Payment service providers wishing to allow the designated third party to fulfil the reporting obligations in a consolidated way (i.e. by presenting one single report referred to several payment service providers affected by the same major operational or security incident) should inform the competent authority in the home Member State, include the contact

information included under 'Affected PSP' in the template and make certain that the following conditions are satisfied:

a. Include this provision in the contract underpinning the delegated reporting.

b. Make the consolidated reporting conditional on the incident's being caused by a disruption in the services provided by the third party.

c. Confine the consolidated reporting to payment service providers established in the same Member State.

d. Ensure that the third party assesses the materiality of the incident for each affected payment service provider and includes in the consolidated report only those payment service providers for which the incident is classified as major. Furthermore, ensure that, in case of doubt, a payment service provider is included in the consolidated report as long as there is no evidence that it should not.

e. Ensure that, when there are fields of the template where a common answer is not possible (e.g. section B 2, B 4 or C 3), the third party either (i) fills them out individually for each affected payment service provider, further specifying the identity of each payment service provider to which the information relates, or (ii) uses ranges, in those fields where this is an option, representing the lowest and highest values as observed or estimated for the different payment service providers.

f. Payment service providers should ensure that the third party keeps them informed at all times of all the relevant information regarding the incident and all the interactions that the third party may have with the competent authority and of the contents thereof, but only as far as is compatible with avoiding any breach of confidentiality as regards the information that relates to other payment service providers.

3.3. Payment service providers should not delegate their reporting obligations before informing the competent authority in the home Member State or after having been informed that the outsourcing agreement does not meet the requirements referred to in Guideline 3.1, letter b).

3.4. Payment service providers wishing to withdraw the delegation of their reporting obligations should communicate this decision to the competent authority in the home Member State, in accordance with the deadlines and procedures established by the latter. Payment service providers should also inform the competent authority in the home Member State of any material development affecting the designated third party and its ability to fulfil the reporting obligations.

3.5. Payment service providers should materially complete their reporting obligations without any recourse to external assistance whenever the designated third party fails to inform the competent authority in the home Member State of a major operational or security incident in accordance with Article 96 of PSD2 and with these Guidelines. Furthermore, payment service providers should ensure that an incident is not reported twice, individually by said payment service provider and once again by the third party.

Guideline 4: Operational and security policy

4.1. Payment service providers should ensure that their general operational and security policy clearly defines all the responsibilities for incident reporting under PSD2, as well as the processes implemented to fulfil the requirements defined in the present Guidelines.

5. Guidelines addressed to competent authorities on the criteria on how to assess the relevance of the incident and the details of the incident reports to be shared with other domestic authorities

Guideline 5: Assessment of the relevance of the incident

5.1. Competent authorities in the home Member State should assess the relevance of a major operational or security incident to other domestic authorities, taking as a basis their own expert opinion and using the following criteria as primary indicators of the importance of said incident:

a. The causes of the incident are within the regulatory remit of the other domestic authority (i.e. its field of competence).
b. The consequences of the incident have an impact on the objectives of another domestic authority (e.g. safeguarding of financial stability).
c. The incident affects, or could affect, payment service users on a wide scale.
d. The incident is likely to receive, or has received, wide media coverage.

5.2. Competent authorities in the home Member State should carry out this assessment on a continuous basis during the lifetime of the incident, to identify any possible change that could make an incident relevant that was previously not considered as such.

Guideline 6: Information to be shared

6.1. Notwithstanding any other legal requirement to share incident-related information with other domestic authorities, competent authorities should provide information about major operational or security incidents to the domestic authorities identified following the application of Guideline 5.1 (i.e. 'other relevant domestic authorities'), as a minimum, at the time of receiving the initial report (or, alternatively, the report that prompted the sharing of information) and when they are notified that business is back to normal (i.e. last intermediate report).

6.2. Competent authorities should submit to other relevant domestic authorities the information needed to provide a clear picture of what happened and the potential consequences. To do so, they should provide, as a minimum, the information given by the payment service provider in the following fields of the template (either in the initial or in the intermediate report):

- date and time of detection of the incident;
- date and time of beginning of the incident;
- date and time when the incident was restored or is expected to be restored;
- short description of the incident (including non-sensitive parts of the detailed description);
- short description of measures taken or planned to be taken to recover from the incident;
- description of how the incident could affect other PSPs and/or infrastructures;
- description (if any) of the media coverage;
- cause of the incident.

6.3. Competent authorities should conduct proper anonymisation, as needed, and leave out any information that could be subject to confidentiality or intellectual property restrictions before sharing any incident-related information with other relevant domestic authorities. Nevertheless, competent authorities should provide other relevant domestic authorities with the name and address of the reporting payment service provider when said domestic authorities can guarantee that the information will be treated confidentially.

6.4. Competent authorities should at all times preserve the confidentiality and integrity of the information stored and exchanged with other relevant domestic authorities and also authenticate themselves properly towards other relevant domestic authorities. In particular, competent authorities should treat all information received under these Guidelines in accordance with the professional secrecy obligations set out in PSD2, without prejudice to applicable Union law and national requirements.

6. Guidelines addressed to competent authorities on the criteria on how to assess the relevant details of the incident reports to be shared with the EBA and the ECB and on the format and procedures for their communication

Guideline 7: Information to be shared

7.1. Competent authorities should always provide the EBA and the ECB with all reports received from (or on behalf of) payment service providers affected by a major operational or security incident (i.e. initial, intermediate and final reports).

Guideline 8: Communication

8.1. Competent authorities should at all times preserve the confidentiality and integrity of the information stored and exchanged with the EBA and the ECB and also authenticate themselves properly towards the EBA and the ECB. In particular, competent authorities should treat all information received under these Guidelines in accordance with the professional secrecy obligations set out in PSD2, without prejudice to applicable Union law and national requirements.

8.2. To avoid delays in the transmission of incident-related information to the EBA/ECB and help minimise the risks of operational disruptions, competent authorities should support appropriate means of communication.

Annex 1 – Reporting templates for payment service providers

CLASSIFICATION: RESTRICTED

Major Incident Report

☐ Initial report	within 4 hours after detection
☐ Intermediate report	maximum of 3 business days from previous report
☐ Last intermediate report	
☐ Final report	within 2 weeks after closing the incident
☐ Incident reclassified as non-major — Please explain:	

Report date	DD/MM/YYYY	Time	HH:MM
Incident identification number, if applicable (for interim and final reports)			

A - Initial report

A 1 - GENERAL DETAILS					
Type of report					
Type of report	☐ Individual	☐ Consolidated			
Affected payment service provider (PSP)					
PSP name					
PSP unique identification number, if relevant					
PSP authorisation number					
Head of group, if applicable					
Home country					
Country/countries affected by the incident					
Primary contact person		Email		Telephone	
Secondary contact person		Email		Telephone	
Reporting entity (complete this section if the reporting entity is not the affected PSP in case of delegated reporting)					
Name of the reporting entity					
Unique identification number, if relevant					
Authorisation number, if applicable					
Primary contact person		Email		Telephone	
Secondary contact person		Email		Telephone	

A 2 - INCIDENT DETECTION and INITIAL CLASSIFICATION			
Date and time of detection of the incident	DD/MM/YYYY, HH:MM		
The incident was detected by (1)		If Other, please explain:	
Please provide a short and general description of the incident (should you deem the incident to have an impact in other EU Member States(s), and if feasible within the applicable reporting deadlines, please provide a translation in English)			
What is the estimated time for the next update?	DD/MM/YYYY, HH:MM		

B - Intermediate report

B 1 - GENERAL DETAILS

Please provide a more DETAILED description of the incident. e.g. information on: - What is the specific issue? - How it happened - How did it develop - Was it related to a previous incident? - Consequences (in particular for payment service users) - Background of the incident detection - Areas affected - Actions taken so far - Service providers/ third party affected or involved - Crisis management started (internal and/or external (Central Bank Crisis management)) - PSP internal classification of the incident	
Date and time of beginning of the incident (if already identified)	DD/MM/YYYY, HH:MM
Incident status	☐ Diagnostics ☐ Recovery ☐ Repair ☐ Restoration
Date and time when the incident was restored or is expected to be restored	DD/MM/YYYY, HH:MM

B 2 - INCIDENT CLASSIFICATION & INFORMATION ON THE INCIDENT

Overall impact	☐ Integrity ☐ Confidentiality ☐ Continuity ☐ Availability ☐ Authenticity
Transactions affected [2]	Number of transactions affected — ☐ Actual figure ☐ Estimation As a % of regular number of transactions — ☐ Actual figure ☐ Estimation Value of transactions affected in EUR — ☐ Actual figure ☐ Estimation Comments:
Payment service users affected [3]	Number of payment service users affected — ☐ Actual figure ☐ Estimation As a %-of total payment service users — ☐ Actual figure ☐ Estimation
Service downtime [4]	Total service downtime — DD:HH:MM — ☐ Actual figure ☐ Estimation
Economic impact [5]	Direct costs in EUR — ☐ Actual figure ☐ Estimation Indirect costs in EUR — ☐ Actual figure ☐ Estimation
High level of internal escalation	☐ YES ☐ YES, AND CRISIS MODE (OR EQUIVALENT) IS LIKELY TO BE CALLED UPON ☐ NO Describe the level of internal escalation of the incident, indicating if it has triggered or is likely to trigger a crisis mode (or equivalent) and if so, please describe
Other PSPs or relevant infrastructures potentially affected	☐ YES ☐ NO Describe how this incident could affect other PSPs and/or infrastructures
Reputational impact	☐ YES ☐ NO Describe how the incident could affect the reputation of the PSP (e.g. media coverage, potential legal or regulatory infringement, etc.)

B 3 - INCIDENT DESCRIPTION

Type of Incident	☐ Operational ☐ Security
Cause of incident	☐ Under investigation ☐ External attack ☐ Internal attack → Type of attack: ☐ Distributed/Denial of Service (D/DoS) ☐ Infection of internal systems ☐ Targeted intrusion ☐ Other If Other, specify ☐ External events ☐ Human error ☐ Process failure ☐ System failure ☐ Other — If Other, specify
Was the incident affecting you directly, or indirectly through a service provider?	☐ Directly ☐ Indirectly — If indirectly, please provide the service provider's name

B 4 - INCIDENT IMPACT

Building(s) affected (Address), if applicable	
Commercial channels affected	☐ Branches ☐ Telephone banking ☐ Point of sale ☐ E-banking ☐ Mobile banking ☐ Other ☐ ATMs If Other, specify:
Payment services affected	☐ Cash placement on a payment account ☐ Credit transfers ☐ Money remittance ☐ Cash withdrawal from a payment account ☐ Direct debits ☐ Payment initiation services ☐ Operations required for operating a payment account ☐ Card payments ☐ Account information services ☐ Acquiring of payment instruments ☐ Issuing of payment instruments ☐ Other If Other, specify:
Functional areas affected	☐ Authentication/authorisation ☐ Clearing ☐ Indirect settlement ☐ Communication ☐ Direct settlement ☐ Other If Other, specify:
Systems and components affected	☐ Application/software ☐ Hardware ☐ Database ☐ Network/infrastructure ☐ Other If Other, specify:
Staff affected	☐ YES ☐ NO Describe how the incident could affect the staff of the PSP/service provider (e.g. staff not being able to reach the office to support customers, etc.)

B 5 - INCIDENT MITIGATION

Which actions/measures have been taken so far or are planned to recover from the incident?	
Has the Business Continuity Plan and/or Disaster Recovery Plan been activated?	☐ YES ☐ NO
If so, when?	DD/MM/YYYY, HH:MM
If so, please describe	
Has the PSP cancelled or weakened some controls because of the incident?	☐ YES ☐ NO
If so, please explain	

C - Final report	
If no intermediate report has been sent, please also complete section B	
C 1 - GENERAL DETAILS	
Please update the information from the intermediate report (summary): - additional actions/measures taken to recover from the incident - final remediation actions taken - root cause analysis - lessons learnt - addittional actions - any other relevant information	
Date and time of closing the incident	DD/MM/YYYY, HH:MM
If the PSP had to cancel or weaken some controls because of the incident, are the original controls back in place?	☐ YES ☐ NO
If so, please explain	
C 2 - ROOT CAUSE ANALYSIS AND FOLLOW-UP	
What was the root cause (if already known)? (possible to attach a file with detailed information)	
Main corrective actions/measures taken or planned to prevent the incident from happening again in the future, if already known	
C 3 - ADDITIONAL INFORMATION	
Has the incident been shared with other PSPs for information purposes?	☐ YES ☐ NO
If so, please provide details	
Has any legal action been taken against the PSP?	☐ YES ☐ NO
If so, please provide details	

Notes:

(1) Pull-down menu: payment service user; internal organisation; external organisation; none of the above

(2) Pull-down menu: > 10% of regular level of transactions and > EUR 100,000; > 25% of regular level of transactions or > EUR 5 milion; none of the above

(3) Pull-down menu: > 5,000 and > 10% payment service users; > 50,000 or > 25% payment service users; none of the above

(4) Pull-down menu: > 2 hours; < 2 hours

(5) Pull-down menu: > Max (0,1% Tier 1 capital, EUR 200,000) or > EUR 5 million; none of the above

CONSOLIDATED REPORT - LIST OF PSPs		
PSP Name	**PSP Unique Identification Number**	**PSP Authorisation number**

INSTRUCTIONS FOR FILLING OUT THE TEMPLATES

Payment service providers should fill out the relevant section of the template, depending on the reporting phase they are in: section A for the initial report, section B for intermediate reports and section C for the final report. All fields are mandatory, unless it is clearly specified otherwise.

Headline

Initial report: this is the first notification that the PSP submits to the competent authority in the home Member State.

Intermediate report: this is an update of a previous (initial or intermediate) report on the same incident.

Last intermediate report: this informs the competent authority in the home Member State that regular activities have been recovered and business is back to normal, so no more intermediate reports will be submitted.

Final report: it is the last report the PSP will send on the incident, since (i) a root cause analysis has already been carried out and estimations can be replaced with real figures or (ii) the incident is not considered major any more.

Incident reclassified as non-major: the incident no longer fulfils the criteria to be considered major and is not expected to fulfil them before it is resolved. PSPs should explain the reasons for this downgrading.

Report date and time: exact date and time of submission of the report to the competent authority.

Incident identification number, if applicable (for intermediate and final report): the reference number issued by the competent authority at the time of the initial report to uniquely identify the incident, if applicable (i.e. if such a reference is provided by the competent authority).

A – Initial report

A 1 – General details

Type of report:

Individual: the report refers to a single PSP.

Consolidated: the report refers to several PSPs making use of the consolidated reporting option. The fields under 'Affected PSP' should be left blank (with the exception of the field 'Country/countries affected by the incident') and a list of the PSPs included in the report should be provided by filling in the corresponding table (Consolidated report – List of PSPs).

Affected PSP: refers to the PSP that is experiencing the incident.

PSP name: full name of the PSP subject to the reporting procedure as it appears in the applicable official national PSP registry.

PSP unique identification number, if relevant: the relevant unique identification number used in each Member State to identify the PSP, to be provided by the PSP if the field 'PSP authorisation number' is not filled in.

PSP authorisation number: home Member State authorisation number.

Head of group: in case of groups of entities as defined in Article 4(40) of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) 1093/2010 and repealing Directive 2007/64/EC, please indicate the name of the head entity.

Home country: Member State in which the registered office of the PSP is situated; or if the PSP has, under its national law, no registered office, the Member State in which its head office is situated.

Country/countries affected by the incident: country or countries where the impact of the incident has materialised (e.g. several branches of a PSP located in different countries are affected). It may or may not be the same as the home Member State.

Primary contact person: first name and surname of the person responsible for reporting the incident or, if a third party reports on behalf of the affected PSP, first name and surname of the person in charge of the incident management/risk department or similar area, at the affected PSP.

Email: email address to which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate email.

Telephone: telephone number to call with any requests for further clarifications, if needed. It can be either a personal or a corporate phone number.

Secondary contact person: first name and surname of an alternative person who could be contacted by the competent authority to inquiry about an incident when the primary contact person is not available. If a third party reports on behalf of the affected PSP, first name and surname of an alternative person in the incident management/risk department or similar area, at the affected PSP.

Email: email address of the alternative contact person to which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate email address.

Telephone: telephone number of the alternative contact person to call with any requests for further clarifications, if needed. It can be either a personal or a corporate phone number.

Reporting entity: this section should be completed if a third party fulfils the reporting obligations on behalf of the affected PSP.

Name of the reporting entity: full name of the entity that reports the incident, as it appears in the applicable official national business registry.

Unique identification number, if relevant: the relevant unique identification number used in the country where the third party is located to identify the entity that is reporting the incident, to be provided by the reporting entity if the field 'Authorisation number' is not filled in.

Authorisation number, if applicable: the authorisation number of the third party in the country where it is located, when applicable.

Primary contact person: first name and surname of the person responsible for reporting the incident.

Email: email address to which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate email.

Telephone: telephone number to call with any requests for further clarifications, if needed. It can be either a personal or a corporate phone number.

Secondary contact person: first name and surname of an alternative person in the entity that is reporting the incident who could be contacted by the competent authority when the primary contact person is not available.

Email: email address of the alternative contact person to which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate email address.

Telephone: telephone number of the alternative contact person to call with any requests for further clarifications could be addressed, if needed. It can be either a

personal or a corporate phone number.

A 2 – Incident detection and initial classification

Date and time of detection of the incident: date and time at which the incident was first identified.

Incident detected by: indicate whether the incident was detected by a payment service user, some other party from within the PSP (e.g. internal audit function) or an external party (e.g. external service provider). If it was none of those, please provide an explanation in the corresponding field.

Short and general description of the incident: please explain briefly the most relevant issues of the incident, covering possible causes, immediate impacts, etc.

What is the estimated time for the next update?: indicate the estimated date and time for the submission of the next update (interim or final report).

B – Intermediate report

B 1 – General details

More detailed description of the incident: please describe the main features of the incident, covering at least the points featured in the questionnaire (what specific issue the PSP is facing, how it started and developed, possible connection with a previous incident, consequences, especially for payment service users, etc.).

Date and time of beginning of the incident: date and time at which the incident started, if known.

Incident status:

Diagnostics: the characteristics of the incident have just been identified.

Repair: the attacked items are being reconfigured.

Recovery: the failed items are being restored to their last recoverable state.

Restoration: the payment-related service is being provided again.

Date and time when the incident was restored or is expected to be restored: indicate the date and time when the incident was or is expected to be under control and business was or is expected to be back to normal.

B 2 – Incident classification/Information on the incident

Overall impact: please indicate which dimensions have been affected by the incident. Multiple boxes may be ticked.

Integrity: the property of safeguarding the accuracy and completeness of assets (including data).

Availability: the property of payment-related services being accessible and usable by payment service users.

Confidentiality: the property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Authenticity: the property of a source being what it claims to be.

Continuity: the property of an organisation's processes, tasks and assets needed for the delivery of payment-related services being fully accessible and running at acceptable predefined levels.

Transactions affected: PSPs should indicate which thresholds are or will probably be reached by the incident, if any, and the related figures: number of transactions affected, percentage of transactions affected in relation to the number of payment transactions carried out with the

same payment services that have been affected by the incident, and total value of the transactions. PSPs should provide specific values for these variables, which may be either actual figures or estimations. Entities reporting on behalf of several PSPs (i.e. consolidated reporting) may provide value ranges instead, representing the lowest and highest values observed or estimated within the group of PSPs included in the report, separated by a hyphen. As a general rule, PSPs should understand as 'transactions affected' all domestic and cross-border transactions that have been or will probably be directly or indirectly affected by the incident and, in particular, those transactions that could not be initiated or processed, those for which the content of the payment message was altered, and those that were fraudulently ordered (whether the funds have been recovered or not). Furthermore, PSPs should understand the regular level of payment transactions to be the daily annual average of domestic and cross-border payment transactions carried out with the same payment services that have been affected by the incident, taking the previous year as the reference period for calculations. If PSPs do not consider this figure to be representative (e.g. because of seasonality), they should use another, more representative, metric instead and convey to the competent authority the underlying rationale for this approach in the field 'Comments'.

Payment service users affected: PSPs should indicate which thresholds are or will probably be reached by the incident, if any, and the related figures: total number of payment service users that have been affected and percentage of payment service users affected in relation to the total number of payment service users. PSPs should provide concrete values for these variables, which may be either actual figures or estimations. Entities reporting on behalf of several PSPs (i.e. consolidated reporting) may provide value ranges instead, representing the lowest and highest values observed or estimated within the group of PSPs included in the report, separated by a hyphen. PSPs should understand as 'payment service users affected' all customers (either domestic or from abroad, consumers or corporates) that have a contract with the affected payment service provider that grants them access to the affected payment service, and that have suffered or will probably suffer the consequences of the incident. PSPs should resort to estimations based on past activity to determine the number of payment service users that may have been using the payment service during the lifetime of the incident. In the case of groups, each PSP should consider only its own payment service users. In the case of a PSP offering operational services to others, that PSP should consider only its own payment service users (if any), and the PSPs receiving those operational services should also assess the incident in relation to their own payment service users. Furthermore, PSPs should take as the total number of payment service users the aggregated figure of domestic and cross-border payment service users contractually bound to them at the time of the incident (or, alternatively, the most recent figure available) and with access to the affected payment service, regardless of their size or whether they are considered active or passive payment service users.

Service downtime: PSPs should indicate if the threshold is or will probably be reached by the incident and the related figure: total service downtime. PSPs should provide concrete values for this variable, which may be either actual figures or estimations. Entities reporting on behalf of several PSPs (i.e. consolidated reporting) may provide a value range instead, representing the lowest and highest values observed or estimated within the group of PSPs included in the report, separated by a hyphen. PSPs should consider the period of time that any task, process or channel related to the provision of payment services is or will probably be down and, thus, prevents (i) the initiation and/or execution of a payment service and/or (ii) access to a payment account. PSPs should count the service downtime from the moment the downtime starts, and they should consider both the time intervals when they are open for business as required for the execution of payment services as well as the closing hours and maintenance periods, where relevant and applicable. If payment service providers are unable to determine when the service

downtime started, they should exceptionally count the service downtime from the moment the downtime is detected.

Economic impact: PSPs should indicate if the threshold is or will probably be reached by the incident and the related figures: direct costs and indirect costs. PSPs should provide concrete values for these variables, which may be either actual figures or estimations. Entities reporting on behalf of several PSPs (i.e. consolidated reporting) may provide a value range instead, representing the lowest and highest values observed or estimated within the group of PSPs included in the report, separated by a hyphen. PSPs should consider both the costs that can be connected to the incident directly and those which are indirectly related to the incident. Among other things, PSPs should take into account expropriated funds or assets, replacement costs of hardware or software, other forensic or remediation costs, fees due to non-compliance with contractual obligations, sanctions, external liabilities and lost revenues. As regards the indirect costs, PSPs should consider only those that are already known or very likely to materialise.

> **Direct costs:** amount of money (euro) directly cost by the incident, including funds needed to rectify the incident (e.g. expropriated funds or assets, replacement costs of hard- and software, fees due to non-compliance with contractual obligations).
>
> **Indirect costs:** amount of money (euro) indirectly cost by the incident (e.g. customer redress/compensation costs, revenues lost as a result of missed business opportunities, potential legal costs).

High level of internal escalation: PSPs should consider whether or not, as a result of its impact on payment-related services, the Chief Information Officer (or similar position) has been or will probably be informed about the incident outside any periodical notification procedure and on a continuous basis throughout the lifetime of the incident. In the case of delegated reporting, the escalation would take place within the third party. Furthermore, PSPs should consider whether or not, as a result of the impact of the incident on payment-related services, a crisis mode has been or is likely to be triggered.

Other PSPs or relevant infrastructures potentially affected: payment service providers should assess the impact of the incident on the financial market, understood as the financial market infrastructures and/or card payment schemes that support it and the rest of the PSPs. In particular, PSPs should assess whether or not the incident has been or will probably be replicated at other PSPs, whether or not it has affected or will probably affect the smooth functioning of financial market infrastructures and whether or not it has compromised or will probably compromise the solidity of the financial system as a whole. PSPs should bear in mind various dimensions such as whether the component/software affected is proprietary or generally available, whether the compromised network is internal or external and whether or not the PSP has stopped or will probably stop fulfilling its obligations in the financial market infrastructures of which it is a member.

Reputational impact: PSPs should consider the level of visibility that, to the best of their knowledge, the incident has gained or will probably gain in the marketplace. In particular, PSPs should consider the likelihood that the incident will cause harm to society as a good indicator of its potential to affect their reputation. PSPs should take into account whether or not (i) the incident has affected a visible process and is therefore likely to receive or has already received media coverage (considering not only traditional media, such as newspapers, but also blogs, social networks, etc.), (ii) regulatory obligations have been or are likely to be missed, (iii) sanctions have been or are likely to be breached or (iv) the same type of incident has occurred before.

B 3 – Incident description

Type of Incident: indicate whether, to the best of your knowledge, it is an operational or a security incident.

Operational: incident stemming from inadequate or failed processes, people and systems or events of force majeure that affect the integrity, availability, confidentiality, authenticity and/or continuity of payment-related services.

Security: unauthorised access, use, disclosure, disruption, modification or destruction of the PSP's assets that affect the integrity, availability, confidentiality, authenticity and/or continuity of payment-related services. This may happen when, among other things, the PSP experiences cyberattacks, inadequate design or implementation of security policies, or inadequate physical security.

Cause of incident: indicate the cause of the incident or, if it is not known yet, the one that it is most likely to be. Multiple boxes may be ticked.

Under investigation: the cause has not been determined yet.

External attack: the source of the cause comes from outside, and is intentionally targeting the PSP (e.g. malware attacks).

Internal attack: the source of the cause comes from inside, and is intentionally targeting the PSP (e.g. internal fraud).

Type of attack:

Distributed/Denial of Service (D/DoS): an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.

Infection of internal systems: harmful activity that attacks computer systems, trying to steal hard disk space or CPU time, access private information, corrupt data, spam contacts, etc.

Targeted intrusion: unauthorised act of spying, snooping and stealing information through cyberspace.

Other: any other type of attack the PSP may have suffered, either directly or through a service provider. In particular, if there has been an attack aimed at the authorisation and authentication process, this box should be ticked. Details should be added in the free text field.

External events: the cause is associated with events generally outside the organisation's control (e.g. natural disasters, legal issues, business issues and service dependencies).

Human error: the incident was caused by the unintentional mistake of a person, be it as part of the payment procedure (e.g. uploading the wrong payments batch file to the payments system) or related to it somehow (e.g. the power is accidentally cut off and the payment activity is put on hold).

Process failure: the cause of the incident was poor design or execution of the payment process, the process controls and/or the supporting processes (e.g. process for change/migration, testing, configuration, capacity, monitoring).

System failure: the cause of the incident is associated with inadequate design, execution, components, specifications, integration or complexity of the systems that support the payment activity.

Other: the cause of the incident is none of the above. Further details should be provided in the free text field.

Was the incident affecting you directly, or indirectly through a service provider?: an incident can target a PSP directly or affect it indirectly, through a third party. In the case of an indirect impact, please provide the name of the service provider(s).

B 4 – Incident impact

Building(s) affected (Address), if applicable: if a physical building is affected, please indicate its address.

Commercial channels affected: indicate the channel or channels of interaction with payment service users that have been affected by the incident. Multiple boxes may be ticked.

Branches: place of business (other than the head office) which is a part of a PSP, has no legal personality and carries out directly some or all of the transactions inherent in the business of a PSP. All of the places of the business set up in the same Member State by a PSP with a head office in another Member State should be regarded as a single branch.

E-banking: the use of computers to carry out financial transactions over the internet.

Telephone banking: the use of telephones to carry out financial transactions.

Mobile banking: the use of a specific banking application on a smartphone or similar device to carry out financial transactions.

ATMs: electromechanical devices that allow payment service users to withdraw cash from their accounts and/or access other services.

Point of sale: physical premise of the merchant at which the payment transaction is initiated.

Other: the commercial channel affected is none of the above. Further details should be provided in the free text field.

Payment services affected: indicate those payment services that are not working properly as a result of the incident. Multiple boxes may be ticked.

Cash placement on a payment account: the handing of cash to a PSP to credit it on a payment account.

Cash withdrawal from a payment account: the request received by a PSP from its payment service user to provide cash and debit his/her payment account by the corresponding amount.

Operations required for operating a payment account: those actions needed to be performed in a payment account to activate, deactivate and/or maintain it (e.g. opening, blocking).

Acquiring of payment instruments: a payment service consisting in a PSP contracting with a payee to accept and process payment transactions, which results in a transfer of funds to the payee.

Credit transfers: a payment service for crediting a payee's payment account with a payment transaction or a series of payment transactions from a payer's payment account by the PSP which holds the payer's payment account, based on an instruction given by the payer.

Direct debits: a payment service for debiting a payer's payment account, where a payment transaction is initiated by the payee on the basis of the consent given by the payer to the payee, to the payee's payment service provider or to the payer's own payment service provider.

Card payments: a payment service based on a payment card scheme's infrastructure and business rules to make a payment transaction by means of any card, telecommunication, digital or IT device, or software if this results in a debit or a credit card transaction. Card-based payment transactions exclude transactions based on other kinds of payment services.

Issuing of payment instruments: a payment service consisting in a PSP contracting with a payer to provide her with a payment instrument to initiate and process the payer's payment transactions.

Money remittance: a payment service whereby funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another PSP acting on behalf of the payee, and/or whereby such funds are received on behalf of and made available to the payee.

Payment initiation services: payment services to initiate a payment order at the request of the payment service user with respect to a payment account held at another PSP.

Account information services: online payment services to provide consolidated information on one or more payment accounts held by the payment service user with either another PSP or more than one PSP.

Other: the payment service affected is none of the above. Further details should be provided in the free text field.

Functional areas affected: indicate the step or steps of the payment process that have been affected by the incident. Multiple boxes may be ticked.

Authentication/authorisation: procedures which allow the PSP to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials and the payment service user (or a third party acting on behalf of that user) giving his/her consent to transfer funds or securities.

Communication: flow of information for the purpose of identification, authentication, notification and information between the account-servicing PSP and payment initiation service providers, account information service providers, payers, payees and other PSPs.

Clearing: a process of transmitting, reconciling and, in some cases, confirming transfer orders prior to settlement, potentially including the netting of orders and the establishment of final positions for settlement.

Direct settlement: the completion of a transaction or of processing with the aim of discharging participants' obligations through the transfer of funds, when this action is carried out by the affected PSP itself.

Indirect settlement: the completion of a transaction or of processing with the aim of discharging participants' obligations through the transfer of funds, when this action is carried out by another PSP on behalf of the affected PSP.

Other: the functional area affected is none of the above. Further details should be provided in the free text field.

Systems and components affected: indicate which part or parts of the PSP's technological infrastructure have been affected by the incident. Multiple boxes may be ticked.

Application/software: programs, operating systems, etc. that support the provision of payment services by the PSP.

Database: data structure which stores personal and payment information needed to execute payment transactions.

Hardware: physical technology equipment that runs the processes and/or stores the data needed by PSPs to carry out their payment-related activity.

Network/infrastructure: telecommunications networks, either public or private, that allow the exchange of data and information during the payment process (e.g. the internet).

Other: the system and component affected is none of the above. Further details should be provided in the free text field.

Staff affected: indicate whether or not the incident has had any effects on the PSP's staff and, if so, provide details in the free text field.

B 5 – Incident mitigation

Which actions/measures have been taken so far or are planned to recover from the incident?: please provide details about actions that have been taken or planned to be taken to temporarily address the incident.

Have the Business Continuity Plans and/or Disaster Recovery Plans been activated?: please indicate whether or not and, if so, provide the most relevant details of what happened (i.e. when they were activated and what these plans consisted of).

Has the PSP cancelled or weakened some controls because of the incident?: please indicate whether or not the PSP has had to override some controls (e.g. stop using the four eyes principle) to address the incident and, if so, provide details of the underlying reasons justifying the weakening or cancelling of controls.

C – Final report

C 1 – General details

Update of the information from the intermediate report (summary): please provide further information on the actions taken to recover from the incident and avoid its recurrence, analysis of the root cause, lessons learnt, etc.

Date and time of closing the incident: indicate the date and time when the incident was considered closed.

Are the original controls back in place?: if the PSP had to cancel or weaken some controls because of the incident, indicate whether or not such controls are back in place and provide any additional information in the free text field.

C 2 – Root cause analysis and follow-up

What was the root cause, if already known?: please explain which is the root cause of the incident or, if it is not known yet, the preliminary conclusions drawn from the root cause analysis. PSPs may attach a file with detailed information if considered necessary.

Main corrective actions/measures taken or planned to prevent the incident from happening again in the future, if already known: please describe the main actions that have been taken or are planned to be taken to prevent a future reoccurrence of the incident.

C 3 – Additional information

Has the incident been shared with other PSPs for information purposes?: please provide an overview of which PSPs have been contacted, either formally or informally, to debrief them about the incident, providing details of the PSPs that have been informed, the information that has been shared and the underlying reasons for sharing this information.

Has any legal action been taken against the PSP?: please indicate whether or not, at the time of filling out the final report, the PSP has suffered any legal action (e.g. been taken to court or lost its licence) as a result of the incident.