

Major Incident Report - INSTRUCTIONS TO FILL OUT THE TEMPLATE

0. Please enable VBA macros to ensure the correct functioning of the tool: File -> Options -> Trust Center -> Trust Center Settings -> Enable all macros -> OK. You may need to close Excel and open the file again.
1. 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.
1. Payment service providers should use the same file when submitting the initial, intermediate and final reports related to the same incident. **All fields are mandatory, unless it is clearly specified otherwise.**
2. Please, select the type of report:

Type of report submitted	Report that is being submitted	Deadlines	Explanatory notes
<u>Initial report</u>	<input type="checkbox"/>	within 4 hours after classification	The initial report is the first notification that the PSP submits to the competent authority in the home Member State.
<u>Intermediate report</u>	<input type="checkbox"/>	maximum of 3 working days from the submission of the initial report	The intermediate report provides a more detailed description of the incident and its consequences. It is an update of the initial report (and where applicable to a previous intermediate report) on the same incident. It informs the competent authority in the home Member State that regular activities have been recovered and business is back to normal.
<u>Final report</u>	<input type="checkbox"/>	within 20 working days after the submission of the intermediate report	The final report 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 anymore and need to be reclassified.
<u>Incident reclassified as non-major</u>			An incident reclassified as non-major refers when it does not longer fulfil the criteria to be considered major and is not expected to fulfil them before it is solved. PSPs should explain the reasons for this reclassification.

Major Incident Report

Initial report	within 4 hours after classification of the incident as major
----------------	--

Initial report	within 4 hours after classification of the incident as major
----------------	--

--

--

A - Initial report

A 1 - GENERAL DETAILS

Type of report	Number of reports	Percentage of reports
...

Type of report	
----------------	--

Affected payment service provider (PSP)	
---	--

PSP name	
----------	--

PSP national identification number	
------------------------------------	--

Head of group, if applicable	
------------------------------	--

<input type="checkbox"/> AT	<input type="checkbox"/> DE	<input type="checkbox"/> FR	<input type="checkbox"/> IS	<input type="checkbox"/> LV	<input type="checkbox"/> PT
<input type="checkbox"/> BE	<input type="checkbox"/> DK	<input type="checkbox"/> GR	<input type="checkbox"/> IT	<input type="checkbox"/> MT	<input type="checkbox"/> RO
<input type="checkbox"/> BG	<input type="checkbox"/> EE	<input type="checkbox"/> HR	<input type="checkbox"/> LI	<input type="checkbox"/> NL	<input type="checkbox"/> SE
<input type="checkbox"/> CY	<input type="checkbox"/> ES	<input type="checkbox"/> HU	<input type="checkbox"/> LT	<input type="checkbox"/> NO	<input type="checkbox"/> SI
<input type="checkbox"/> CZ	<input type="checkbox"/> FI	<input type="checkbox"/> IE	<input type="checkbox"/> LU	<input type="checkbox"/> PL	<input type="checkbox"/> SK

--

--	--

--	--

--

[illegible]

--	--

Reporting entity (complete this section if the reporting entity is not the affected PSP in case of delegated reporting)									
---	--	--	--	--	--	--	--	--	--

Name of the reporting entity	
------------------------------	--

National identification number	
--------------------------------	--

[illegible]

--	--

--	--

[illegible]

--	--

--	--

A 2 - INCIDENT DETECTION and CLASSIFICATION									
---	--	--	--	--	--	--	--	--	--

Date and time of detection of the incident (DD/MM/YYYY HH:MM)	
---	--

Date and time of classification of the incident (DD/MM/YYYY HH:MM)	
--	--

▼

--	--

▼

☐ Transactions affected ☐ Payment service users affected ☐ Service downtime ☐ Breach of security of network or information ☐ Economic impact ☐ High level of internal escalation ☐ Other PSPs or relevant infrastructures potentially affected ☐ Reputational impact

<p> </p>	<p> </p>	<p> </p>
----------	----------	----------

A short and general description of the incident	
---	--

[illegible]

In case the reporting is done on a consolidated basis, please complete the following table:

[illegible]

Major Incident Report

Intermediate report

maximum of 3 working days from the submission of the initial report

Report date (DD/MM/YYYY)

Time (HH:MM)

Incident reference code

B - Intermediate report

B 1 - GENERAL DETAILS

More detailed description of the incident:

What is the specific issue?

How did the incident start?

How did it evolve?

What are the consequences (in particular for payment service users)?

Was the incident communicated to payment service users?

▼

If 'Yes', please specify:

Was it related to a previous incident/s?

▼

If 'Yes', please specify:

Were other service providers/third parties affected or involved?

▼

If 'Yes', please specify:

Was crisis management started (internal and/or external)?

▼

If 'Yes', please specify:

Date and time of beginning of the incident (if already identified) (DD/MM/YYYY HH:MM)

Date and time when the incident was restored or is expected to be restored (DD/MM/YYYY HH:MM)

Functional areas affected

☐ Authentication/Authorisation

☐ Direct settlement

☐ Communication

☐ Indirect settlement

☐ Clearing

☐ Other

If 'Other', please specify:

Changes made to previous reports

B 2 - INCIDENT CLASSIFICATION / INFORMATION ON THE INCIDENT			
Transactions affected ⁽²⁾	Impact level	<div></div>	
	Number of transactions affected	<div></div>	<div></div>
	As a % of regular number of transactions	<div></div>	<div></div>
	Value of transactions affected in EUR	<div></div>	<div></div>
	Duration of the incident (only applicable to operational incidents)	<div></div>	<div></div>
	Comments:	<div></div>	
Payment service users affected ⁽³⁾	Impact level	<div></div>	
	Number of payment service users affected	<div></div>	<div></div>
	As a % of total payment service users	<div></div>	<div></div>
Breach of security of network or information systems	<div></div>		
	Describe how the network or information systems have been affected		<div></div>
Service downtime	<div></div>	Days:	Hours: Minutes: <div></div>
	Total service downtime:		<div></div> <div></div> <div></div> <div></div>
Economic impact	Impact level	<div></div>	
	Direct costs in EUR	<div></div>	<div></div>
	Indirect costs in EUR	<div></div>	<div></div>
High level of internal escalation	<div></div>		
	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		<div></div>
Other PSPs or relevant infrastructures potentially affected	<div></div>		
	Describe how this incident could affect other PSPs and/or infrastructures		<div></div>
Reputational impact	<div></div>		
	Describe how the incident could affect the reputation of the PSP (e.g. media coverage, publication of legal actions or infringements of law...)		<div></div>

B 3 - INCIDENT DESCRIPTION			
Type of Incident	<div></div>		
Cause of incident	<div><input type="checkbox"/> Under investigation <input type="checkbox"/> Malicious action <input type="checkbox"/> Process failure <input type="checkbox"/> System failure <input type="checkbox"/> Human errors <input type="checkbox"/> External events <input type="checkbox"/> Other</div>		
	If 'Other', please specify:		
Was the incident affecting you directly, or indirectly through a service provider?	<div></div>	If 'Indirectly', please provide the service provider's name:	
B 4 - INCIDENT IMPACT			
Overall impact	<div><input type="checkbox"/> Integrity <input type="checkbox"/> Availability <input type="checkbox"/> Confidentiality <input type="checkbox"/> Authenticity</div>		
Commercial channels affected	<div><input type="checkbox"/> Branches <input type="checkbox"/> E-banking <input type="checkbox"/> E-commerce <input type="checkbox"/> Telephone banking <input type="checkbox"/> Mobile banking <input type="checkbox"/> ATMs <input type="checkbox"/> Point of sale <input type="checkbox"/> Other</div>		
	If 'Other', please specify:		
Payment services affected	<div><input type="checkbox"/> Cash placement on a payment account <input type="checkbox"/> Cash withdrawal from a payment account <input type="checkbox"/> Operations required for operating a payment account <input type="checkbox"/> Acquiring of payment instruments <input type="checkbox"/> Credit transfers <input type="checkbox"/> Direct debits <input type="checkbox"/> Card payments <input type="checkbox"/> Issuing of payment instruments <input type="checkbox"/> Money remittance <input type="checkbox"/> Payment initiation <input type="checkbox"/> Account information services</div>		
B 5 - INCIDENT MITIGATION			
Which actions/measures have been taken so far or are planned to recover from the incident?			
Have the Business Continuity Plan and/or Disaster Recovery Plan been activated?	<div></div>		
If so, when? (DD/MM/YYYY HH:MM)			
If so, please describe			

Major Incident Report

Please select the type of report:

within 20 working days after the submission of the intermediate report

Please describe:

(applicable for incidents reclassified as non-major)

Report date (DD/MM/YYYY)

Time (HH:MM)

Incident reference code

C - Final report

If no intermediate report has been sent, please complete also section B

C 1 - GENERAL DETAILS

Update of the information from the initial report and the intermediate report(s)

Changes made to previous reports

asdfas

Any other relevant information

Are all original controls in place?

If "No", specify which controls and the additional period required for their restoration

C 2 - ROOT CAUSE ANALYSIS AND FOLLOW UP

What was the root cause (if already known)?

☐ Malicious action

☐ Process failure

☐ System failure

☐ Human error

☐ External event

☐ Other

Please specify:

☐ Malicious code

☐ Information gathering

☐ Intrusions

☐ Distributed/Denial of service attack (D/DoS)

☐ Deliberate internal actions

☐ Deliberate external physical damage

☐ Information content security

☐ Fraudulent actions

☐ Other

☐ Deficient monitoring and control

☐ Communication issues

☐ Improper operations

☐ Inadequate Change management

☐ Inadequacy of internal procedures and documentation

☐ Recovery issues

☐ Other

☐ Hardware failure

☐ Network failure

☐ Database issues

☐ Software/application failure

☐ Physical damage

☐ Other

☐ Unintended

☐ Inaction

☐ Insufficient resources

☐ Other

☐ Failure of a supplier/technical service provider

☐ Force majeure

☐ Other

If 'Other', please specify:

Other relevant information on the root cause

Main corrective actions/measures taken or planned to prevent the incident from happening again in the future, if already known

C 3 - ADDITIONAL INFORMATON

Has the incident been shared with other PSPs for information purposes?

If 'Yes', please provide details:

Has any legal action been taken against the PSP?

If 'Yes', please provide details:

Assessment of the effectiveness of the action taken

Please provide details: