

Major Incident Report									
Initial report					Reset dropdown selections				
Report date (DD/MM/YYYY)					Time (HH:MM)				
Incident reference code									
A - Initial report									
A 1 - GENERAL DETAILS									
Type of report									
Type of report									
Affected payment service provider (PSP)									
PSP name									
PSP national identification number									
Head of group, if applicable									
Country / countries affected by the incident									
☐ AT ☐ BE ☐ BG ☐ CY ☐ CZ ☐ DE ☐ DK ☐ EE ☐ ES ☐ FI ☐ FR ☐ GR ☐ HR ☐ HU ☐ IE ☐ IS ☐ IT ☐ LI ☐ LT ☐ LU ☐ LV ☐ MT ☐ NL ☐ NO ☐ PL ☐ PT ☐ RO ☐ SE ☐ SI ☐ SK									

Major Incident Report

Intermediate report

Reset dropdown
selections

Report date (DDMMYYYY)

Incident reference code

Time (HHMM)

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) (DDMMYYYY HH:MM)

Date and time when the incident was restored or is expected to be

restored (DDMMYYYY 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

Number of transactions affected

As a % of regular number of transactions

Value of transactions affected in EUR

Duration of the incident (only applicable to operational incidents)

Comments:

Payment service users affected ⁽³⁾

Impact level

Number of payment service users affected

As a % of total payment service users

Breach of security of network or information systems

Describe how the network or information systems have been affected

Service downtime

Impact level

Total service downtime:

Days:

Hours:

Minutes:

Economic impact

Impact level

Direct costs in EUR

Indirect costs in EUR

High level of internal escalation

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

Impact level

Describe how this incident could affect other PSPs

and/or infrastructures

Reputational impact

Impact level

Describe how the incident could affect the reputation of the PSP (e.g. media coverage, publication of legal actions or infringements of law...)

B 3 - INCIDENT DESCRIPTION

Type of Incident

Cause of incident

☐ Under investigation☐ Malicious action☐ Process failure☐ System failure☐ Human errors☐ External events☐ Other

If 'Other', please specify:

Was the incident affecting you directly, or indirectly through a service provider?

If 'Indirectly', please provide the service provider's name:

B 4 - INCIDENT IMPACT

Overall impact

☐ Integrity☐ Availability☐ Confidentiality☐ Authenticity

Commercial channels affected

☐ Branches☐ E-banking☐ E-commerce☐ Telephone banking☐ Mobile banking☐ ATMs☐ Point of sale☐ Other

If 'Other', please specify:

Payment services affected

☐ Cash placement on a payment account☐ Cash withdrawal from a payment account☐ Operations required for operating a payments account☐ Acquiring of payment instruments☐ Credit transfers☐ Direct debits☐ Card payments☐ Issuing of payment instruments☐ Money remittance☐ Payment initiation☐ Account information services

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?

If so, when? (DDMMYYYY HH:MM)

If so, please describe

Major Incident Report	
-----------------------	--

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						
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	
Other relevant information on the root cause	If "Other", please specify:					
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?						
Has any legal action been taken against the PSP?						
Assessment of the effectiveness of the action taken						