

Reporting template on major incidents
(anglická verze uvedeného dokumentu)

Major Incident Report									
☐	Initial report								
☐	Intermediate report								
☐	Last intermediate report								
☐	Final report								
☐	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: a) What is the specific issue? b) How it happened c) How did it develop d) Was it related to a previous incident? e) Consequences (in particular for payment service users) f) Background of the incident detection g) Areas affected h) Actions taken so far i) Service providers/ third party affected or involved j) Crisis management started (internal and/or external (Central Bank Crisis management)) k) 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 As a % of regular number of transactions Value of transactions affected in EUR Comments: ☐ Actual figure ☐ Estimation ☐ Actual figure ☐ Estimation ☐ Actual figure ☐ Estimation		
Payment service users affected ⁽²⁾	Number of payment service users affected As a % of total payment service users ☐ Actual figure ☐ Estimation ☐ Actual figure ☐ Estimation		
Service downtime ⁽²⁾	Total service downtime DD:HH:MM ☐ Actual figure ☐ Estimation		
Economic impact ⁽²⁾	Direct costs in EUR Indirect costs in EUR ☐ Actual figure ☐ Estimation ☐ 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 ☐ External events ☐ Human error ☐ Process failure ☐ System failure ☐ Other ☐ If Other, specify ☐ Type of attack: ☐ Distributed/Denial of Service (D/DoS) ☐ Infection of internal systems ☐ Targeted intrusion ☐ Other ☐ If Other, specify		
Was the incident affecting you directly, or indirectly through a service provider?	☐ Directly ☐ Indirectly If indirectly, please provide the service providers 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		
Payment services affected	☐ Cash placement on a payment account ☐ Cash withdrawal from a payment account ☐ Operations required for operating a payment account ☐ Acquiring of payment instruments ☐ Credit transfers ☐ Direct debits ☐ Card payments ☐ Issuing of payment instruments ☐ Money remittance ☐ Payment initiation services ☐ Account information services ☐ Other		
Functional areas affected	☐ Authentication/authorisation ☐ Communication ☐ Clearing ☐ Direct settlement ☐ Indirect settlement ☐ Other		
Systems and components affected	☐ Application/software ☐ Database ☐ Hardware ☐ Network/infrastructure ☐ Other		
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): a) additional actions/measures taken to recover from the incident b) final remediation actions taken c) root cause analysis d) lessons learnt e) additional actions f) 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? If so, please explain			☐ YES NO							
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? If so, please provide details			☐ YES NO							
Has any legal action been taken against the PSP? If so, please provide details			☐ YES NO							
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										