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. 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
Initial report	☐	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.
Intermediate report	☐	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.
Final report	☐	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.
Incident reclassified as non-major			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**

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
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						
National identification number						
Primary contact person		Email		Telephone		
Secondary contact person		Email		Telephone		

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*)			
The incident was detected by		If 'Other', please specify:	
Type of Incident			
Criteria triggering the major incident report	☐ 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		
A short and general description of the incident			
Impact in other EU Member States, if applicable			
Reporting to other authorities		If 'Yes', please specify:	
Reasons for late submission of the initial report			

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

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

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				
	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		Days:	Hours:	Minutes:	
	Total service downtime:				
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		Describe how this incident could affect other PSPs and/or infrastructures			
Reputational impact		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 payment 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? *(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 action	Process failure	System failure	Human error	External event
Malicious code	Deficient monitoring and control	Hardware failure	Unintended	Failure of a supplier/technical service provider
Information gathering	Communication issues	Network failure	Inaction	Force majeure
Intrusions	Improper operations	Database issues	Insufficient resources	Other
Distributed/Denial of service attack (D/DoS)	Inadequate Change management	Software/application failure	Other	
Deliberate internal actions	Inadequacy of internal procedures and documentation	Physical damage		
Deliberate external physical damage	Recovery issues	Other		
Information content security	Other			
Fradulent actions				
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: