The mandatory fields for each report are marked in the following colours.

First report	○	*within 4 hours after the incident has been classified as "major"*
Interim report	○	*after the incident closing or within 3 working days after the First report*
Final report	○	*within 20 working days after closing the incident*

Report date and time

Incident ID (for interim or final report)

Changes made to previous reports

Incident reclassified as non-major ☐

Reclassification - Please explain

Operational or security incident report - Payment and Electronic Money Institutions

FIRST REPORT

GENERAL DETAILS

Affected entity - ABI code					
Affected entity - Name					
Contact person within the institution for updates		Email		Phone	
Second contact person within the institution for updates		Email		Phone	

Country/countries affected by the incident

IT - Italy ☐	CY - Cyprus ☐	EE - Estonia ☐	GR - Greece ☐	IS - Iceland ☐	LV - Latvia ☐	PL - Poland ☐	SI - Slovenia ☐
AT - Austria ☐	CZ - Czech Republic ☐	ES - Spain ☐	HR - Croatia ☐	LI - Liechtenstein ☐	MT - Malta ☐	PT - Portugal ☐	SK - Slovakia ☐
BE - Belgium ☐	DE - Germany ☐	FI - Finland ☐	HU - Hungary ☐	LT - Lithuania ☐	NL - Netherlands ☐	RO - Romania ☐	Other (Extra UE) ☐
BG - Bulgaria ☐	DK - Denmark ☐	FR - France ☐	IE - Ireland ☐	LU - Luxembourg ☐	NO - Norway ☐	SE - Sweden ☐	

INCIDENT DETECTION AND CLASSIFICATION

Date and time of detection of the incident			
Date and time of classification of the incident		Reasons for late submission first report	
Incident was detected by		If Other, please specify:	
Type of incident			

Criteria triggering the major incident report *(multiple selections possible)*

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

Impact in other EU Member States, if applicable			
Reporting to other authorities	○ Yes ○ No	If 'Yes', please specify:	

A short and general description of the incident
Please provide a general description of the incident
Explain briefly the most relevant issues of the incident, covering possible causes, immediate impacts, etc.

INTERIM REPORT

GENERAL DETAILS

What is the specific issue?	
How did the incident start?	
How did it evolve?	
What are the consequences? Please provide a detailed description of the consequences,especially for payment service users	

Was the incident communicated to payment service users?	○ Yes ○ No	If Yes, please specify:	
Was it related to a previous incident/s?	○ Yes ○ No	If Yes, please specify:	
Date and time of beginning of the incident - if known			
Is the incident closed?	○ Yes ○ No	Please enter the date/time when the incident was closed or is expected to be closed	

CLASSIFICATION OF THE INCIDENT / INFORMATION ON THE INCIDENT

Cause of incident *(multiple selections possible)*	Malicious actions ☐	Human errors ☐	Other ☐	If Other, please specify:	
	Process failure ☐	External events ☐			
	System failure ☐	Under investigation ☐			

Transactions affected	Impact level			
	Number of transactions affected		Actual or estimated	Comments:
	As a % of regular number of transactions		Actual or estimated	
	Value of transactions affected in EUR		Actual or estimated	
	Duration of the incident (only applicable to operational incidents)		Actual or estimated	
Payment service users affected	Impact level			
	Number of users affected		Actual or estimated	
	As a % total service users		Actual or estimated	

Breach of security of network or information systems		
	If Yes, describe how the network or information systems have been affected	
Service downtime		
	Total service downtime	Days: Hours Minutes:: Actual or estimated

Economic impact	Impact level		
	Direct financial loss in EUR		Actual or estimated
	Indirect financial loss in EUR		Actual or estimated

High level of internal escalation		
	If yes, please specify	
Was crisis management started (internal and/or external)?		
	If yes, please specify	
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...)	
Were any legal or regulatory requirements breached?		
	If yes, please specify	
Other entities (e.g., intermediaries, infrastructures) involved or potentially interested?		
	Describe how this incident affect or could affect other intermediaries and/or infrastructures	

INCIDENT IMPACT AND INCIDENT MITIGATION

Overall impact (multiple selections possible)	Integrity ☐	Availability ☐	Confidentiality ☐	Authenticity ☐
Was the incident affecting you directly, or indirectly through a service provider?	Directly ◯	Through a service provider ◯	If indirectly,please provide the service provider's name	
Were other service providers/third parties affected or involved?	◯ Yes ◯ No	If Yes, please specify:		
Commercial channels affected (multiple selections possible)	Branches ☐	Telephone banking ☐	Point of sale ☐	E-Commerce ☐
	E-banking ☐	Mobile banking ☐	ATM ☐	Other ☐
	If Other, please specify:			
Payment services affected (multiple selections possible)	Cash placement on a payment account ☐	Credit transfers ☐	Money remittance ☐	Acquiring of payment instruments ☐
	Cash withdrawal from a payment account ☐	Direct debits ☐	Payment initiation services ☐	Issuing of payment instruments ☐
	Operations for operating a payment account ☐	Card payments ☐	Account information services ☐	
Payment services functional areas affected (multiple selections possible)	Authentication/Authorization ☐	Clearing ☐	Indirect settlement ☐	
	Communication ☐	Direct settlement ☐	Other ☐	If Other, please specify:
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 and how?	◯ Yes ◯ No	Date and time:	Please, describe	

FINAL REPORT

GENERAL DETAILS

Any other relevant information Please update the information from the interim report and add any relevant addittional information/actions			
Are all original controls in place?		If "No", specify which controls and the additional period required for their restoration	

ROOT CAUSE - FOLLOW UP AND ADDITIONAL INFORMATION

What was the root cause (if already known)? (multiple selections possible)	Malicious Action ☐	Process failure ☐	System failure ☐	Human error ☐	External event ☐
Please specify (multiple selections possible)	Malicious code ☐	Deficient monitoring and control ☐	Hardware failure ☐	Unintended ☐	Failure of a supplier/technical service provider ☐
	Information gathering ☐	Communication issues ☐	Network failure ☐	Inaction ☐	
	Intrusions ☐	Improper operations ☐	Database issues ☐	Insufficient resources ☐	Force majeure ☐
	DoS/DDoS ☐	Change management ☐	Software/application failure ☐	Others (please specify) ☐	Others (please specify) ☐
	Deliberate internal actions ☐	Inadequacy of internal procedures and documentation ☐	Physical damage ☐		
	Deliberate external physical damage ☐		Others (please specify) ☐		
	Information context security ☐	Recovery issues ☐			
	Fraudolent action ☐	Others (please specify) ☐			
	Others (please specify) ☐		If Other, please specify:		
	Other root cause (please specify) ☐				
Other relevant information on the root cause					
Main corrective actions/measures taken/planned to prevent the incident from happening again in the future, if known					
Has the incident been shared with other financial intermediaries (or CertFIN) for information purposes?	◯ Yes ◯ No	If Yes, please specify			
Has any legal action been taken against the group?	◯ Yes ◯ No	If Yes, please specify			
Assessment of the effectiveness of the action taken		Please provide details			