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

Initial report	***within 4 hours after the incident detection***
Interim report	***within 3 business days after the previous***
Last interim report	***report after the incident closing***
Final report	***within 2 weeks after closing the incident***

Report date and time

Incident ID (for interim or final report)

Estimated time for the next update

Next update - please explain

Incident reclassified as non-major

Incident reclassified as non-major - please explain

Operational or security incident report - Payment and Electronic Money Institutions

GENERAL DETAILS

PSP name	
ABI code (5 digits)	
Authorization number (numero di iscrizione Albo)	
Country/countries affected by the incident	
Contact person within the institution for updates	
Second contact person for updates	
Incident detection date and time	
The incident was detected by	
Date/time of beginning of the incident (if known)	
Incident status	
Is the incident closed?	Yes / No

Email
Email
Telephone
Telephone

If other, please specify

Please enter the date/time when the incident was closed or is expected to be closed

DESCRIPTION OF THE INCIDENT

Type of Incident	
Initial report 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 Please provide a detailed description of the incident Include information (if known and/or applicable) - What is the specific issue? -Background to incident detection, who was involved, what happened, how the incident was discovered, how it developed -Attacker(s), cause of the incident, Affected areas/systems and impact -Channels affected, Consequences (in particular for customers) -Was it related to a previous incident? -Actions taken so far -Specify whether a third party/outsourced provider was affected (name of the provider affected, how it was affected) and how the supervised entity was impacted -Crisis management -Internal classification of the incident	
Final report Please update the information from the interim report and add details of: -Additional actions/measures taken to recover from the incident -Technical vulnerability exploited (provide CVE number if known) -Entry vector -Internal escalation / crisis management / relevant actions taken -The investigation (external parties involved) -(Final) remediation actions taken -Additional security controls applied as a result of the incident -Lessons learned, Root cause analysis -Any relevant additional actions -Any other relevant information	

INFORMATION ON THE INCIDENT

Was the incident affecting you directly, or through a service provider?	○ Directly ○ Through a service provider — If indirectly,please provide the service provider's name:
Type of incident - cyber *(multiple selections possible)*	**Malware** ☐ — Ransomware ☐ / Trojan horse ☐ / Virus/worm ☐ / Mobile malware ☐ **Social engineering** ☐ — Phishing / *ishing ☐ / Spear phishing ☐ / Pretexting ☐ / Other "social engineering" ☐ **Insider/Third Party Provider Threat** ☐ — Accidental data leakage/corruption ☐ / Intentional misuse of access rights - by insider ☐ / Intent. misuse access rights - by external providers ☐ **Unauthorised access** ☐ — "Brute force" Attack ☐ / Malicious script injection - OS commanding ☐ / Other exploited vulnerability ☐ **Denial of service** ☐ **Other** ☐ If other, please specify: IIncident classified as an Advanced Persistent Threat? ☐
Type of incident - operational incident *(multiple selections possible)*	Accidental (e.g. human error) ☐ * with the exclusion of "Accidental data leakage/corruption", classified as cyber incidents Process failure ☐ SW problem ☐ HW or infrastructural problem ☐ Sabotage (physical attack) ☐ Natural event - disaster ☐ Other ☐ If other, please specify:

CLASSIFICATION AND IMPACT OF THE INCIDENT

Overall impact *(multiple selections possible)*	Integrity ☐	Availability ☐	Confidentiality ☐ / Authenticity ☐ / Continuity ☐
Transactions affected	Number of transactions affected		Actual figure ○ Estimation ○
	As a % of regular number of transactions		Actual figure ○ Estimation ○
	Value of transactions affected in EUR		Actual figure ○ Estimation ○
	Comments		
Users affected	Number of users affected		Actual figure ○ Estimation ○
	As a % total service users		Actual figure ○ Estimation ○
Service downtime	Total service downtime	GG:HH:MM	Actual figure ○ Estimation ○
Economic impact	Direct financial loss in EUR		Actual figure ○ Estimation ○
	Indirect financial loss in EUR		Actual figure ○ Estimation ○
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 entities (e.g., intermediaries, infrastructures) involved or potentially interested? (systemic impact)	Describe how this incident affect or could affect other intermediaries and/or infrastructures		
Were any legal or regulatory requirements breached?	If yes, please specify		
Is there any reputational impact?	Describe how the incident could affect the reputation of the PSP (e.g. media coverage, potential legal or regulatory infringement, etc.)		
Other impacts (if any)			

DETAILS ON THE IMPACT OF THE INCIDENT

Building(s) affected (Address), if applicable	
Systems affected *(multiple selections possible)*	Applications/software ☐ Hardware ☐ Database ☐ Network/infrastructure ☐ Other ☐ If other, please specify
Commercial channels affected *(multiple selections possible)*	Branches ☐ Phone banking ☐ Point of sale ☐ Other ☐ E-banking ☐ Mobile banking ☐ ATM ☐ If other, please specify
Payment services affected *(multiple selections possible)*	Cash placement on a payment account ☐ Credit transfers ☐ Money remittance ☐ Cash withdrawal from a payment account ☐ Direct debits ☐ Payment initiation services ☐ Operations for operating a payment account ☐ Card payments ☐ Account information services ☐ Acquiring of payment instruments ☐ Issuing of payment instruments ☐ Other ☐ If other, please specify
Payment services functional areas affected *(multiple selections possible)*	Authentication/Authorization ☐ Clearing ☐ Indirect settlement ☐ Communication ☐ Direct settlement ☐ Other ☐ If other, please specify
Staff affected	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.)

INVESTIGATION, MITIGATION AND RESOLUTION OF THE INCIDENT

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? If so, when? If so, please describe	○ Yes ○ No	Date and time:	Please describe
Has the PSP cancelled or weakened some controls because of the incident?	○ Yes ○ No	If yes, please describe	
If some controls had been canceled or weakened because of the incident, are the original controls back in place?	○ Yes ○ No	If yes, please describe	
What was the root cause? (possible to attach a file with detailed information))			
Main corrective actions/measures taken/ planned to prevent the incident from happening again in the future, if already known			
Was the incident reported to the national CERT/CSIRT?	○ Yes ○ No		
Has the incident been shared with other financial PSP for information purposes? With the CertFin? If so, provide details	○ Yes ○ No	If yes, please describe	
Has any legal action been taken against the group? If so, please provide details	○ Yes ○ No	If yes, please describe	