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

First report	○	***within 2 hours after the incident has been classified as "significant"***
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-significant ☐

Reclassification - Please explain

Operational or security incident report - Significant Institutions

FIRST REPORT

GENERAL DETAILS

Reporting entity - ABI code					
Reporting entity - JST code					
Reporting 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			
Does the incident affect entity's payment services?	○ Yes ○ No		

Reason for reporting the incident
(multiple selections possible)

Transactions affected - High impact ☐

Crisis management procedures triggered or is likely to be called upon ☐

Estimated financial impact is above EUR 5M or max (0.1% of CET1 capital; 200.000 EUR) ☐

High internal escalation (e.g. Chief Information Officer or equivalent) ☐

Incident is likely to lead to breaches of legal or regulatory obligations ☐

Users affected - High impact ☐

Incident is reported to the national CERT/ CSIRT, security agency or police (only cyber) ☐

Incident publicly reported and/or can cause significant reputational damage ☐

Incident may affect other institutions/organisations (systemic impact) ☐

The significance assessment does not lead to a clear outcome so the incident ☐

Combination of multiple minor impacts ☐

Transactions affected - Low impact ☐

Users affected - Low impact ☐

Service downtime ☐

Breach of security of network or information systems ☐

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? Please provide a detailed description of how incident started, including (if known and/or applicable): -Background to incident detection, who was involved, what happened, how the incident was discovered, how it developed -Attacker(s), cause of the incident	
How did it evolve?	
What are the consequences? Please provide a detailed description of the consequences, including (if known and/or applicable): -Affected areas/systems and impact -Channels affected, Consequences (in particular for users) -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 -Internal classification of the incident	

Was the incident communicated to payment service users?	○ Yes ○ No ○ N.A.	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 action ☐
- Process failure ☐
- System failure ☐
- Human errors ☐
- External events ☐
- Under investigation ☐
- Other ☐

If Other, please specify:

Incident category
(only for Cyber incidents)
(multiple selections possible)

Malware ☐	Social engineering ☐	Insider/Third Party Provider Threat ☐	Unauthorised access ☐	
Ransomware ☐	Phishing / *ishing ☐	Accidental data leakage/corruption ☐	Brute force attack ☐	Denial of service ☐
Trojan horse ☐	Spear phishing ☐	Intentional misuse of access rights:	Malicious script injection and/or OS commanding ☐	Scanning or sniffing ☐
Virus/worm/Spyware ☐	Pretexting ☐	by insider ☐	Other exploited vulnerability ☐	Other ☐
Mobile malware ☐	Other social engineering ☐	by service provider ☐	Unauthorized use of resources, copyright ☐	
			Account/application compromise ☐	
			Unauthorized access to/modification of information ☐	

If Other, please specify:

Incident classified as an Advanced Persistent Threat? ☐

Information regarding the attacker(s)
(only for Cyber incidents)
(multiple selections possible)

Terrorists ☐	Hacktivists ☐	Unknown ☐
Foreign agencies - state-sponsored hackers ☐	Inside job/Unaware employee ☐	Other ☐
Other hackers (e.g. criminals, script kiddies, etc) ☐		

If Other, please specify:

Transactions affected
(only when payment services are interested)

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		

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		
Was the incident escalated internally to senior (top) management for action outside of day-to-day procedures?					
	If yes, please specify				
Were crisis management (or equivalent) procedures activated or is it likely activated?					
	If yes, please specify				
Were any legal or regulatory requirements breached?					
	If yes, please specify				
Was there any media coverage?					
	If yes, please specify the media/newspapers /blogs that covered the topic				
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:*			
Other impacts	Unauthorised release of information? ☐	Online banking fraud? ☐			
	Information related to the institution leaked? ☐	Other impact? ☐			
	Sensitive client information leaked? ☐	If other, please specify			
Services and components affected (multiple selections possible)	Endpoints/clients (laptops, PCs, OSs, user applications, etc) ☐	Banking-related user application/ software (sales, trading, credit, etc.) ☐	Networking and telecommunications (firewalls, routers, switches, PBX, etc) ☐	Data management & storage (fileservers, databases, data warehouses, etc.) ☐	
	Enterprise software applications (SAP, Oracle, etc) ☐	Internet platforms (webservers, application servers, etc) ☐	Other ☐	If Other, please specify:	
Business lines affected (multiple selections possible)	Corporate Finance ☐	Trading & Sales ☐	Retail Banking ☐	Commercial Banking ☐	Other ☐
	Payment & Settlement ☐	Agency Services ☐	Asset Management ☐	Retail Brokerage ☐	
	If Other, please specify:				
Commercial channels affected (multiple selections possible)	Branches ☐	Telephone banking ☐	Point of sale ☐	E-Commerce ☐	
	E-banking ☐	Mobile banking ☐	ATMs ☐	Other ☐	
	If Other, please specify:				
Payment services affected (if any) (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 (if any) (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?					
Was a business continuity plan activated? If yes, when and how?	○ Yes ○ No	Date and time:		Please, describe	
Was a disaster recovery plan activated? If yes, when and how?	○ Yes ○ No	Date and time:		Please, describe	

FINAL REPORT

GENERAL DETAILS

Additional information 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 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 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

Root cause and/or Vulnerabilities/weaknesses identified (only for Operational incidents) (multiple selections possible)	Deficient monitoring and control ☐	Inadequacy of internal procedures and documentation ☐	Database issues ☐	Human inaction ☐	Deliberate internal actions ☐
	Communication issues ☐	Recovery issues ☐	Software/application failure ☐	Insufficient human resource ☐	Deliberate external physical damage ☐
	Improper operations ☐	Hardware failure ☐	Physical damage ☐	Force majeure ☐	Other ☐
	Inadequate Change management ☐	Network failure ☐	Unintentional human activity ☐	Failure of a supplier/technical service provider ☐	If Other, please specify:
Root cause and/or Vulnerabilities/weaknesses identified *(only for Cyber incidents)* *(multiple selections possible)*	Inadequate patch management ☐	Inadequate security configurations for secure hardware and software on devices, laptops, workstations, servers ☐	Inadequate application sw security controls (web-based and other appl.) ☐	Inadequate identity access management ☐	Lack of staff awareness and/or compliance ☐
	Unauthorised software/wrong version ☐	Inadequate boundary defences ☐	Inadequate DDoS defences ☐	Inadequate maintenance and monitoring of logs ☐	Other ☐
	Inadequate privileged account manag. ☐	Inadequate control of network ports, protocols and services ☐	Inadequate penetration and security testing ☐	Inadequate malware defences ☐	If Other, please specify:
	Inadequate email/web browser protection ☐	Inadequate resilience and/or back-up of systems or files ☐	Inadequate network segmentation ☐	Unsecured network devices (firewalls, routers, switches) ☐	
Other relevant information on the root cause					
What was the entry vector of the incident? (only for Cyber incidents) (multiple selections possible)	Website ☐ Instant messaging ☐ Phone ☐	E-mail ☐ Third party network ☐ Unauthorised devices ☐	Lost / stolen devices ☐ Chat rooms / social media ☐ Abuse of Administrative Privileges ☐	Other ☐ If Other, please specify	
Main corrective actions/measures taken/planned to prevent the incident from happening again in the future, if already known					
Who is leading the investigation of the incident?					
Who is leading the remediation actions?					
Police/other security agencies involved in the investigation?	○ Police ○ Other ○ None				
Was the incident reported to the national CERT/CSIRT?	○ Yes ○ No				
Has the incident been shared with other financial intermediaries for information purposes? And with the CertFIN?	○ 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			

LIST OF AFFECTED ENTITIES

Entity name	ABI (or other Unique Identification number)	COUNTRY	TYPE OF ENTITY AFFECTED