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	○	***within 3 working days after the previous report***
Last Interim 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-significant ☐

Reclassification - Please explain ____

Information security incident report - Significant Institutions

GENERAL DETAILS

Reporting entity - JST code					
Reporting entity - ABI code					
Reporting entity - Registration number					
Country/countries affected by the incident					
Contact person within the institution for updates		Email		Phone	
Second contact person within the inst. for updates		Email		Phone	
Incident detection date and time					
Incident discovered by				If Other, please specify:	
Date/time of beginning of the incident (if known)					
Incident status					
Is the incident closed?	○ Yes ○ No			Please enter the date/time when the incident was closed or is expected to be closed	

DESCRIPTION OF THE INCIDENT

Incident category	
Does the incident affect entity's payment services?	○ Yes ○ No
First 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 started (internal and/or external -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 -Lessons learnt -Any relevant addittional actions -Any other relevant information	

INFORMATION ON THE INCIDENT

Was the incident affecting you directly, or indirectly through a service provider?	○ Direclty	○ Through a service provider	If indirectly,please provide the service provider's name		
Incident type - cyber *(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 / OS commanding ☐	
	Virus/worm ☐	Pretexting ☐	by insider ☐	Other exploited vulnerability ☐	Other ☐
	Mobile malware ☐	Other social engineering ☐	by service provider ☐		
	If Other, please specify:				
	Incident classified as an Advanced Persistent Threat? ☐				
Incident type - Operational (*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:				
Information regarding the attacker(s) *(only for Cyber incidents)*	Terrorists ☐	Hacktivists ☐	Unknown ☐		
	Foreign agencies - state-sponsored hackers ☐	Inside job/Unaware employee ☐	Other ☐		
	Other hackers (criminals, script kiddies, etc) ☐				
	If Other, please specify:				

IMPACT OF THE INCIDENT & REASON FOR REPORTING

Overall impact (multiple selections possible)	Integrity ☐	Availability ☐	Confidentiality ☐	Authenticity ☐	Continuity ☐
Transactions affected *(only when payment services are interested)*					
	Number of transactions affected		Actual ○	Estimated ○	
	As % of regular number of transactions		Actual ○	Estimated ○	
	Value of transactions affected in EUR		Actual ○	Estimated ○	
	Comments				
Users affected					
	Number of users affected As a		Actual ○	Estimated ○	
	% of total service users		Actual ○	Estimated ○	
Disruption of critical service?					
	Total service downtime	DD:HH:MM	Actual ○	Estimated ○	
Economic impact					
	Direct financial loss in EUR		Actual ○	Estimated ○	
	Indirect financial loss in EUR		Actual ○	Estimated ○	
Was the incident escalated internally to senior (top) management for action outside of day-to-day procedures?					
	If yes, please specify (e.g., tt group level CIO, CISO, COO, CRO, CEO, ExCo, ExBoard				
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
Other impacts	Unauthorised release of information? ☐ Information related to the institution leaked? ☐ Sensitive client information leaked? ☐ Defacing / data alteration ☐ Online banking fraud? ☐ Other frauds ☐ If Other frauds,please specify Other impact? ☐ If yes, please specify
Reason for reporting the incident *(multiple selections possible)*	Incident affects more than 50.000 or 25% of the provider's service users ☐ Incident affects more than 25% of the payment service regular level of transactions (in terms of number of transactions) or EUR 5 Mln ☐ Incident publicly reported and/or can cause significant reputational damage ☐ Crisis management procedures triggered or is likely to be called upon (including cyber insurance) ☐ The estimated financial impact is > Max. (0.1% Tier 1 capital,* EUR 200 000) or EUR 5 million ☐ Combination of multiple minor impacts (#/% customers,#/% transactions, service downtime>2h) - see instructions ☐ Incident was internally escalated up to the Chief Information Officer (or equivalent) outside of regular reporting ☐ Incident may affect other institutions/organisations (systemic impact) ☐ Incident is likely to lead to breaches of legal or regulatory obligations ☐ Incident is reported to the national CERT/CSIRT, security agency or police ☐ The significance assessment does not lead to a clear outcome so the incident is reported ☐
Building(s) affected (Address), if applicable	
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:
Systems affected (multiple selections possible)	Application/software ☐ Hardware ☐ Database ☐ Network/infrastructure ☐ 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 ☐ Phone banking ☐ Point of sale ☐ Other ☐ E-banking ☐ Mobile banking ☐ ATM ☐ If Other, please specify:
Payment services affected (if any)	Cash placement on a payment account ☐ Credit transfers ☐ Money remittance Payment ☐ Cash withdrawal from a payment account ☐ Direct debits ☐ Initiation services Account ☐ Operations for operating a payment account ☐ Card payments ☐ Information services ☐ Acquiring of payment instruments ☐ Issuing of payment instruments ☐ Other ☐ If Other, please specify:
Payment services functional areas affected (if any)(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 intermediary/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?					
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	
Has the intermediary cancelled or weakened some controls because of the incident?	○ Yes ○ No	If yes, please explain:			
Who is leading the investigation of the incident?					
Who is leading the remediation actions?					
If some controls had been canceled/weakened because of the incident, are the original controls back in place?	○ Yes ○ No	If yes, please explain:			
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					
What was the entry vector of the incident (ONLY CYBER)? (multiple selections possible)	Website ☐ Instant messaging ☐ Phone ☐ Abuse of Administrative Privileges ☐	E-mail ☐ Third party network ☐ Unauthorised devices ☐	Lost / stolen devices ☐ Chat rooms / social media ☐ Other ☐		
	If Other, please specify				
Vulnerabilities/weaknesses identified *(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.) ☐	Software bugs ☐	
	Unauthorised software/wrong version ☐	Inadequate boundary defences ☐	Inadequate DDoS defences ☐	Hardware defects ☐	
	Inadequate privileged account manag. ☐	Inadequate control of network ports, protocols and services ☐	Inadequate penetration and security testing ☐	Change management issues ☐	
	nadequate email/web browser protection ☐	Inadequate resilience and/or back-up of systems or files ☐	Inadequate network segmentation ☐	Other procedural issues ☐	
	Inadequate malware defences ☐	Unsecured network devices (firewalls, routers, switches) ☐	Lack of staff awareness and/or compliance ☐	Other ☐	
	Inadequate identity access management ☐	Inadequate maintenance and monitoring of logs ☐			
	If Other, please specify:				
Are the police or other security agencies involved in the investigation?	○ Police ○ Other ○ None				
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? If so, please provide details	○ Yes ○ No	If Yes, please specify			
Has any legal action been taken against the group? If so, please provide details	○ Yes ○ No	If Yes, please specify			

LIST OF AFFECTED ENTITIES

Entity name	ABI (if applicable)	REGISTRATION NUMBER (if applicable)	COUNTRY	TYPE OF ENTITY AFFECTED