Initial report	within 3 hours after detection

Report date	DD/MM/YYYY	Time	HH:MM [1]

A - Initial report

A 1 - GENERAL DETAILS					
Affected entity					
Legal name (1)					
Entity unique identification number, if applicable [3]					
Entity authorisation number, if applicable [4]					
Type of the entity (e.g. RPS processing Instant payments, card payment scheme, etc.)					
Home country of the entity					
Country / countries affected by the incident					
Primary contact person		Email		Telephone	
Secondary contact person		Email		Telephone	
A 2 - INCIDENT DETECTION and INITIAL CLASSIFICATION					
Date and time of detection of the incident	DD/MM/YYYY, HH:MM				
The incident was detected [5]		If other, please explain:			
Please, provide a short and general description of the incident (should you deem the incident to have an impact in other EU Member State(s), and if feasible within the applicable reporting deadlines, please provide a translation in English)					
What is the estimated time for the next update?	DD/MM/YYYY, HH:MM				

Notes:

(1) Hereinafter please indicate also the relevant time zone

(2) Please insert: RPS or Payment Scheme

(3) Please insert the relevant unique identification number used to identify the affected legal entity (e.g. LEI code, national registration number, etc.)

(4) Please insert home Member State authorisation number (in case the affected legal entity is subject to authorisation or licensing for providing services as a RPS/Payment Scheme under the relevant jurisdiction)

(5) Please insert: internally; by external party (e.g. PSP, payment service user, other infrastructure); or none of the above

Major Incident Report

□ First Intermediate report	within 3 business days from previous report
□ Consecutive Intermediate report	

Report date	DD/MM/YYYY	Time	HH:MM [1]
Incident identification number, if applicable [2]			

B - Intermediate report

Please provide also section A

B 1 - GENERAL DETAILS

Detailed description of the incident - e.g. information on: - What is the specific issue? - How it happened? - How did it evolve? - Was it related to a previous incident? - Consequences (in particular for payment service users) - Background of the incident detection - Area's affected - Actions taken so far - Service providers/ third party affected or involved - Crisis management started (internal and/or external (e.g. Lead Overseer Crisis management)) - Internal classification of the incident	
Date and time of beginning of the incident (if already identified)	DD/MM/YYYY, HH:MM
Incident status	□ Diagnostics □ Recovery □ Repair □ Restoration
Date and time when the incident was restored or is expected to be restored	DD/MM/YYYY, HH:MM □ restored □ expected to be restored

B 2 - INCIDENT CLASSIFICATION / INFORMATION ON THE INCIDENT

Overall impact	□ Integrity □ Confidentiality □ Continuity □ Availability □ Authenticity				
Transactions affected		in one single jurisdiction	across the EU		
	Number of transactions affected			□ Actual figure	□ Estimation
	As a % of regular number of transactions			□ Actual figure	□ Estimation
	Duration of the initiation/processing delay			□ Actual figure	□ Estimation
	Comments:				
Participants affected		in one single jurisdiction	across the EU		
	Number of the affected participants			□ Actual figure	□ Estimation
	As a % of total number of participants			□ Actual figure	□ Estimation
Service downtime	Total service downtime	DD:HH:MM		□ Actual figure	□ Estimation
Delayed cut-off	Total duration of cut-off's delay	DD:HH:MM		□ Actual figure	□ Estimation
High level of internal escalation	□ YES □ YES, AND CRISIS MODE (OR EQUIVALENT) IS LIKELY TO BE CALLED UPON □ NO				
	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 FMIs/payment schemes (potentially) affected	□ YES □ NO				
	Describe how this incident could affect other financial market infrastructures				
Reputational impact	□ YES □ NO				
	Describe how the incident could affect the reputation of the entity (e.g. media coverage, potential legal or regulatory infringement…)				

B 3 - INCIDENT DESCRIPTION

Type of Incident	□ Operational □ Security
Cause of incident [3]	□ Under investigation □ External attack □ Internal attack → Type of attack: □ Distributed/Denial of Service (D/DoS) □ Infection of internal systems □ Targeted intrusion □ Other If Other, specify: □ External events □ Human error □ Process failure □ System failure □ Other If Other, specify:
Was the incident affecting the entity directly, or indirectly through a service provider?	□ Directly □ Indirectly If indirectly, please provide the service provider's name:

B 4 - INCIDENT IMPACT

Building(s) affected (Address), if applicable	
Payment services affected	□ Credit transfers □ Issuing of payment instruments □ Other □ Direct debits □ Money remittance □ Card payments □ Payment initiation services □ Acquiring of payment instruments □ Account information services If Other, specify:
Functional areas affected	□ Authentication/Authorisation □ Clearing □ Indirect settlement □ Communication □ Direct settlement □ Other If Other, specify:
Systems and components affected	□ Application / Software □ Hardware □ Database □ Network/infrastructure □ Other If Other, specify:
Staff affected	□ YES □ NO Describe how the incident could affect the staff of the entity (e.g. staff not being able to reach the office)

B 5 - INCIDENT MITIGATION

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?	□ YES □ NO
If so, when?	DD/MM/YYYY, HH:MM
If so, please describe	
Has the entity cancelled or weaken some controls because of the incident?	□ YES □ NO
If so, please explain	

Notes:
(1) Hereinafter please indicate also the relevant time zone
(2) The reference number issued by the Lead Overseer at the time of the initial report to uniquely identify the incident, if applicable (i.e. if such a reference is provided by the Lead Overseer)
(3) Multiple choice is allowed

Major Incident Report

□ Final report within 2 weeks after normal business is restored

□ Incident reclassified as non-major Please, explain:

Report date	DD/MM/YYYY	Time	HH:MM [(1)]
Incident identification number, if applicable			

C - Final report

Please provide also section A

If no intermediate report has been sent, please complete also section B

C 1 - GENERAL DETAILS		
Please, update the information from the intermediate report (summary): - additional actions/measures taken to recover from the incident - final remediation actions taken - root cause analysis - lessons learnt - addittional actions - any other relevant information		
Date and time of closing the incident	DD/MM/YYYY, HH:MM	
If the entity had to cancel or weaken some controls because of the incident, are the original controls back in place?	□ YES	□ NO
If so, please explain:		
C 2 - ROOT CAUSE ANALYSIS AND FOLLOW UP		
What was the root cause? (possible to attach a file with detailed information)		
Main corrective actions/measures taken or planned to prevent the incident from happening again in the future:		
C 3 - ADDITIONAL INFORMATON		
Has the incident been shared with other infrastructures for information purposes?	□ YES	□ NO
If so, please provide details:		
Has any legal action been taken against the reporting entity?	□ YES	□ NO
If so, please provide details:		

REPUBLIK ÖSTERREICH BUNDESKANZLERAMT AMTSSIGNATUR

Unterzeichner	serialNumber=932783133,CN=Bundeskanzleramt,C=AT
Datum/Zeit	2023-06-27T13:56:37+02:00
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.bundeskanzleramt.gv.at/verifizierung
Hinweis	Dieses Dokument wurde amtssigniert.