R E P U B L I C OF ALBANIA
BANK OF ALBANIA
SUPERVISORY COUNCIL

DECISION
No. 10, dated 7.2.2024

ON
APPROVAL OF THE GUIDELINE
ON MAJOR INCIDENT REPORTING

In accordance with and pursuant to article 1, paragraph 4, letter "b", article 12, letter "a" and article 43, letter "c" of the law no. 8269, dated 23.12.1997 "On the Bank of Albania", as amended; and article 89 of the law no. 55/2020, dated 30.4.2020 "On payment services", having regard to the proposal from the Supervision Department, the Supervisory Council of the Bank of Albania,

GUIDES:

1. To approve the guideline "On major incident reporting", according to the text attached to this decision.
2. The payment service providers shall be responsible for the implementation of this Decision.
3. The Supervision Department shall be responsible for monitoring the implementation of this Decision.
4. The Governor's Office and the Research Department shall be responsible for the publication of this Decision, in the Official Journal and in the Official Bulletin of the Bank of Albania, respectively.

This Decision shall enter into force on 1 March 2024 and shall be published in the Official Journal.

SECRETARY **CHAIR**

Elvis ÇIBUKU **Gent SEJKO**

1. GENERAL REQUIREMENTS

1.1. The purpose of the guideline

The purpose of this guideline is to define the:

a) criteria for the classification of major operational or security incidents by payment service providers,
b) reporting format and procedures that payment service providers should follow to notify the Bank of Albania, in accordance with paragraph 1 of article 89 of the law "On payment services".

1.2. Subjects of the guideline

Subjects of this guideline are payment service providers as defined in article 3, paragraph 2, letters "a", "b" dhe "c" of the law no. 55/2020, dated 30.4.2020 "On payment services", which hereinafter in this guideline shall be referred as the law "On payment services".

1.3. Scope of application of the guideline

1.3.1 The requirements of this guideline apply to all incidents included under the definition of "major operational or security incident", which covers both external and internal events that could either be malicious or accidental.

1.3.2 This guideline applies also where the major operational or security incident originates from other countries outside the territory of the Republic of Albania (e.g. when an incident originates in the parent company with its headquarter outside the Republic of Albania) and affects the payment services provided by a payment service provider located in the Republic of Albania, either directly (when a payment-related service is carried out by the entity outside the Republic of Albania) or indirectly (e.g. when the capacity of the payment service provider to keep carrying out its payment activity is jeopardised in another way as a result of the incident).

1.3.3 The requirements of this guideline apply also to major incidents affecting functions outsourced by payment service providers to third parties.

1.4. Definitions

1.4.1 The terms used in this guideline shall have the same meaning as those defined in the law "On payment services".

1.4.2 In addition to paragraph 1.4.1, for the purposes of this guideline, the following terms shall apply:

a) "operational or security incident" – is a singular event or a series of linked events unplanned by the payment service provider, which has or will likely have an adverse impact on the integrity, availability, confidentiality and/or authenticity of payment-related services;
b) "integrity" – is the property of safeguarding the accuracy and completeness of assets (including data);

c) "availability" – is the property of payment-related services being fully accessible and usable by payment service users, according to acceptable levels predefined by the payment service provider;
d) "confidentiality" – is the property that information is not made available or disclosed to unauthorised individuals, entities or processes;
e) "authenticity" – is the property of a source being what it claims to be;
f) "payment-related services" – is any business activity within the meaning of point 37 of article 5 of the law "On payment services", and all the necessary technical supporting tasks for the correct provision of payment services.

1.5. Information sharing with other authorities

1.5.1 Bank of Albania after assessing the importance and relevance of a major operational or security incident to other relevant domestic authorities, may share information with them on such major incidents.

2. CRITERIA FOR THE CLASSIFICATION OF THE INCIDENT AS A MAJOR INCIDENT

2.1. Criteria for the classification of the incident as major incident

2.1.1 Payment service providers should classify as major incidents, those operational or security incidents that fulfil:

a) one or more criteria at the "higher impact level" category, or
b) three or more criteria at the "lower impact level" category,

as set out in table 1, point 2.1.4, and following the assessment defined in this guideline.

2.1.2 Payment service providers should assess an operational or security incident against the following criteria and their underlying indicators:

a) *transactions affected by the incident*, for which payment service providers should determine the total value of the transactions affected, as well as the number of payments compromised as a percentage of the regular (usual) level of payment transactions carried out with the affected payment services;

b) *payment service users affected by the incident*, for which payment service providers should determine the number of payment service users affected, both in absolute terms and as a percentage of the total number of payment service users;

c) *breach of security of network or information systems*, for which payment service providers should determine whether any malicious action has compromised the security of network or information systems related to the provision of payment services;

d) *service downtime*, for which payment service providers should determine the period of time during which the service will likely be unavailable for the payment service

user or during which the payment order within the meaning of article 5, point 49 of the law "On payment services", cannot be fulfilled by the payment service provider;

e) *economic impact*, for which payment service providers should determine the monetary costs associated with the incident holistically and take into account both the absolute figure and, when applicable, the relative importance of these costs in relation to the size of the payment service provider (e.g. to the payment service provider's Tier 1 capital);

f) *high level of internal escalation*, for which payment service providers should determine whether this incident has been or will likely be reported to their executive directors;

g) *other payment service providers or relevant infrastructures potentially affected*, for which payment service providers should determine the systemic implications the incident will likely have, i.e. its potential to spill over beyond the initially affected payment service provider to other payment service providers, financial market infrastructures and/or payment schemes;

h) *reputational impact,* for which payment service providers should determine how the incident can undermine users' trust in the payment service provider itself and, more generally, in the underlying service or the market as a whole.

2.1.3 Payment service providers should calculate the value of the indicators according to the following definitions:

a) *transactions affected by the incident,*

as a general rule, imply all domestic and cross-border transactions that have been or will likely be directly or indirectly impacted by the incident and, in particular, those transactions that could not be initiated or processed, those for which the content of the payment message was altered, and those that were fraudulently ordered (have the funds been recovered or not) or where proper execution is prevented or hampered in any other way by the incident.

For operational incidents affecting the ability to initiate and/or process transactions, payment service providers should report only those incidents with a duration longer than 1 (one) hour. The duration of the incident should be measured from the moment the incident occurs, to the moment when regular activities/operations have been recovered to the level of service that was provided prior to the incident.

Payment service providers should consider as regular level of payment transactions, the daily annual average of domestic and cross-border payment transactions carried out with the same payment services that have been affected by the incident, taking the previous year as the reference period for calculations. In case payment service providers do not consider this figure to be representative (e.g. due to seasonality), they should use another more representative metric instead and notify to the Bank of Albania the underlying rationale for this approach, in the corresponding field of the reporting form in the Annex 1 of this guideline.

b) payment service users affected by the incident,

imply all customers (either domestic or from abroad, consumers or corporates) that have a contract with the affected payment service provider that grants them access to the affected payment service, and that have suffered or will likely suffer the consequences of the incident.

Payment service providers should use estimations based on their past activity, in order to determine the number of payment service users that may have been using the payment service during the lifetime of the incident.

In the case of groups, each payment service provider should only consider its own payment service users. In the case of a payment service provider offering operational services to others, that payment service provider should only consider its own payment service users (if any), and the other payment service providers receiving those operational services should assess the incident in relation to their own payment service users.

For operational incidents affecting the ability to initiate and/or process transactions, payment service providers should report only those incidents that affect payment service users with a duration longer than 1 (one) hour. The duration of the incident should be measured from the moment the incident occurs to the moment when regular activities/operations have been recovered to the level of service that was provided prior to the incident.

Payment service providers should take as the total number of payment service users the aggregated figure of domestic and cross-border payment service users, contractually bound with payment service providers at the time of the incident (or, alternatively, use the most recent figure available of the number of payment service users) and with access to the affected payment service, regardless of their size or whether they are considered active or passive payment service users.

c) breach of security of network or information systems

Payment service providers should determine whether any malicious action has compromised the availability, authenticity, integrity or confidentiality of network or information systems (including data) related to the provision of payment services.

d) service downtime,

is the period of time that any task, process or channel related to the provision of payment services is or will likely be down and, thus, prevents the initiation and/or execution of a payment service and/or the access to a payment account. Payment service providers should count the service downtime from the moment the downtime starts, and they should consider both the time intervals when they are open for business as required for the execution of payment services as well as the closing hours and maintenance periods, where relevant and applicable. If payment service providers are unable to determine when the service downtime started, they should exceptionally count the service downtime from the moment the downtime is detected.

e) *economic impact*,

represents both the costs that can be connected to the incident directly and those which are indirectly related to the incident. For the purposes of measuring/calculating the economic impact, payment service providers should take into account expropriated funds or assets, replacement costs of hardware or software, other legal or remediation costs, fees due to non-compliance with contractual obligations, sanctions, external liabilities and lost revenues. As regards the indirect costs, payment service providers should only consider those that are already known or very likely to materialize.

f) high level of internal escalation

Payment service providers should consider whether, as a result of the impact on payment-related services, the management bodies have been or will likely be informed about the incident, outside any periodical (ad-hoc) notification and on a continuous basis throughout the lifetime of the incident. Payment service providers should consider whether, as a result of the impact of the incident on payment-related services, a crisis mode has been or is likely to be triggered.

g) other payment service providers or relevant infrastructures potentially affected by the incident

Payment service providers should assess the impact of the incident on the financial market, understood as the financial market infrastructures and/or payment schemes that support it and the rest of payment service providers. In particular, payment service providers should assess whether the incident has been or will likely be replicated at other payment service providers, whether it has affected or will likely affect the smooth functioning of financial market infrastructures or whether it has compromised or will likely compromise the sound operation of the financial system as a whole. Payment service providers should consider various dimensions such as whether the component/software affected is proprietary or generally available, whether the compromised network is internal or external or whether the payment service provider has stopped or will likely stop fulfilling its obligations in the financial market infrastructures it is a member of (participant).

h) reputational impact

Payment service providers should consider the level of visibility that, to the best of their knowledge, the incident has gained or will likely gain in the marketplace. In particular, payment service providers should consider the likelihood of the incident causing harm to society as a good indicator of its potential to impact their reputation. Payment service providers should take into account whether:

i. payment service users and/or other payment service providers have complained about the adverse impact of the incident;
ii. the incident has impacted a visible payment service related process and is therefore likely to receive or has already received media coverage (considering not only traditional media, such as newspapers, but also blogs, social networks, etc.);

iii. contractual obligations have been or will likely be missed, resulting in the publication of legal actions against the payment service provider;
iv. regulatory requirements have not been complied with, resulting in the imposition of supervisory measures or sanctions that have been or will likely be made publicly available; and
v. a similar type of incident has occurred before.

2.1.4 Payment service providers should assess an incident by determining, for each individual criterion, whether the relevant thresholds in Table 1 are or will likely be reached before the incident is solved.

Table 1. Thresholds

Criteria (Elements)	Lower impact level	Higher impact level
Transactions affected by the incident	> 10% of the payment service provider's regular level of transactions (in terms of number of transactions) **and** duration of the incident > 1 hour[1] **or** > the equivalent amount in lek of 500,000 euro **and** duration of the incident > 1 hour[1]	> 25% of the payment service provider's regular level of transactions (in terms of number of transactions) **or** > the equivalent amount in lek of 15 million euro
Payment service users affected by the incident	> 5,000 users **and** duration of the incident > 1 hour[1] **or** > 10% of the payment service provider's payment service users **and** duration of the incident > 1 hour[1]	> 50,000 users **or** > 25% of the payment service provider's payment service users
Service downtime	> 2 hours	Not applicable
Breach of security of network or information systems	Yes	Not applicable
Economic impact	Not applicable	> Max (0.1% Tier 1 capital[2], the equivalent amount in lek of 200,000 euro) **or** > the equivalent amount in lek of 5 million euro
High level of internal escalation	Yes	Yes, and a crisis mode (or equivalent) is likely to be triggered
Other payment service providers or relevant infrastructures potentially affected by the incident	Yes	Not applicable
Reputational impact	Yes	Not applicable

[1] The threshold concerning the duration of the incident for a period longer than one hour applies only to operational incidents that affect the ability of the payment service provider to initiate and/or process transactions.

[2] Tier 1 capital as defined in the regulation no. 69/2014 "On the bank's regulatory capital".

2.1.5 Payment service providers should use their estimations if they do not have actual data to support their judgments, as to whether a given threshold is or will likely be reached before the incident is solved (e.g. this could happen during the initial investigation phase of the incident).

2.1.6 Payment service providers should carry out this assessment on a continuous basis during the lifetime of the incident, so as to identify any possible status change, either upwards (from non-major to major incident) or downwards (from major to non-major incident). Any reclassification of the incident from major to non-major should be communicated to the Bank of Albania in line with the requirements set out in the paragraph 3.4.5 of this guideline and without undue delay.

3. NOTIFICATION PROCESS IN THE BANK OF ALBANIA

3.1. Notification process in the Bank of Albania

3.1.1 Payment service providers should collect all relevant information, produce an incident report by completing the form in the Annex 1 of this guideline and submit it to the Bank of Albania. Payment service providers should complete all fields of the form, following the instructions provided in the Annex 1 of this guideline.

3.1.2 Payment service providers should use the same form when submitting to the Bank of Albania the initial, intermediate and final report related to the same incident. Payment service providers should therefore complete a single form in an incremental manner and update, where applicable, the information provided with previous reports.

3.1.3 Payment service providers should further present to the Bank of Albania, if applicable, a copy of the information provided to their users, as foreseen in the paragraph 2 of article 89 of the law "On payment services", as soon as it is available.

3.1.4 Payment service providers should, upon request by the Bank of Albania, provide any additional documents complementing the information submitted with the standardised form. Payment service providers should follow up on any requests from the Bank of Albania to provide additional information or clarifications regarding already submitted documentation.

3.1.5 Any additional information contained in the documents provided by payment service providers to the Bank of Albania, either on the initiative of the payment service provider or upon the request of the Bank of Albania, in line with the paragraph 3.1.4, should be reflected by the payment service provider in the form in the Annex 1 of this guideline.

3.1.6 Payment service providers should at all times preserve the confidentiality and integrity of the information exchanged and their proper authentication towards the Bank of Albania.

3.2. Initial Report

3.2.1 Payment service providers should submit an initial report to the Bank of Albania, after an operational or security incident has been classified as major.

3.2.2 Payment service providers should send the initial report to the Bank of Albania within four hours from the moment the operational or security incident has been classified as major. If the reporting channels of the Bank of Albania are known not to be available or operated at that time, payment service providers should send the initial report as soon as the channels become available/operational again.

3.2.3 Payment service providers should classify the incident in accordance with the paragraph 2.1.1 and 2.1.4 of this guideline in a timely manner after the incident has been detected, but no later than 24 hours after the detection of the incident, and without undue delay after the information required for the classification of the incident is available to the payment service provider. If a longer time is needed to classify the incident, payment service providers should explain in the initial report submitted to the Bank of Albania the relevant reasons.

3.2.4 Payment service providers should also submit an initial report to the Bank of Albania when a previous non-major incident has been reclassified as a major incident. In this particular case, payment service providers should send the initial report to the Bank of Albania immediately after the change of status is identified, or, if the reporting channels of the Bank of Albania are known not to be available or operated at that time, as soon as they become available/operational again.

3.2.5 Payment service providers should provide general information in their initial report (section A of the form), thus presenting some basic characteristics of the incident and its foreseen consequences based on the information available immediately after it was classified as major. Payment service providers should use their estimations when actual data are not available.

3.3. Intermediate Report

3.3.1 Payment service providers should submit to the Bank of Albania the intermediate report, when regular activities have been recovered and business is back to normal, informing the Bank of Albania of this circumstance. Payment service providers should consider business is back to normal, when their activity/operations are restored with the same level of service/conditions as defined by the payment service provider or laid out externally by a service level agreement (processing times, capacity, security requirements, etc.) and when contingency measures are no longer in place. The intermediate report should contain a more detailed description of the incident and its consequences (section B of the form).

3.3.2 If regular activities have not yet been recovered, payment service providers should submit an intermediate report to the Bank of Albania within three working days from the submission of the initial report.

3.3.3 Payment service providers should update the information already provided in sections A and B of the form when they become aware of significant changes since the submission of the previous report (e.g. whether the incident has escalated or decreased, new causes identified or actions taken to fix the problem). This includes the case where the incident has not been resolved within three working days, which would require payment service providers to submit an additional intermediate report to the Bank of Albania. In any case, payment service providers should submit an additional intermediate report at the request of the Bank of Albania.

3.3.4 As in the case of initial reports, when actual data are not available, payment service providers should make use of their estimations.

3.3.5 When business is back to normal before four hours have passed since the incident was classified as major, payment service providers should aim at simultaneously submitting both the initial and the intermediate report (i.e. filling out sections A and B of the form) within the four-hour deadline.

3.4. Final Report

3.4.1 Payment service providers should submit a final report to the Bank of Albania when the root cause analysis has taken place (regardless of whether mitigation measures have already been implemented or the final root cause has been identified) and there are actual figures available to replace any potential estimates carried out by the payment service provider.

3.4.2 Payment service providers should submit the final report to the Bank of Albania in a maximum of 20 working days after business is deemed back to normal. Payment service providers needing an extension of this deadline (e.g. when there are no actual figures on the impact available or the root causes have not been identified yet) should contact the Bank of Albania before the previously mentioned deadline has elapsed and provide an adequate justification for the delay, as well as a new estimated date for submitting the final report.

3.4.3 If payment service providers are able to provide all the information required in the final report (i.e. section C of the form) within the four-hour interval since the incident was classified as major, they should aim at providing simultaneously the information related to initial, intermediate and final reports together.

3.4.4 Payment service providers should include in their final report full information, on the:

a) actual figures on the impact, instead of their estimates (as well as any other update needed in sections A and B of the form); and

b) section C of the form which includes, if already known, the root cause and a summary of measures adopted or planned to be adopted to remove the problem and prevent its reoccurrence in the future.

3.4.5 Payment service providers should also send a final report when, as a result of the continuous assessment of the incident, they identify that an already reported incident no longer fulfils the criteria to be considered as major and is not expected to fulfil

them before the incident is resolved. In this case, payment service providers should send the final report as soon as this circumstance is detected and, in any case, within the deadline for the submission of the next report. In this particular situation, instead of filling out section C of the form, payment service providers should check the box *"incident reclassified as non-major"* and provide an explanation of the reasons justifying this reclassification.

3.5. Reporting through third parties and consolidated reporting

3.5.1 Payment service providers may conclude agreements with third parties for the reporting of major incidents, for which payment service providers inform the Bank of Albania and ensure the fulfillment of the following conditions:

a) the contract or, where applicable, existing internal arrangements within a group (between the group entities), underpinning the reporting through third parties (between the payment service provider and the third party) unambiguously define the allocation of responsibilities of all parties. In particular, the contract/arrangements shall clearly state that, irrespective of the possible transfer of reporting obligations, the affected payment service provider remains fully responsible and accountable for the fulfilment of the requirements set out in article 89 of the law "On payment services" and for the content of the information provided to the Bank of Albania;
b) reporting through third parties complies with the requirements for the transfer of important operational functions as set out in article 21 of the law "On payment services" for payment institutions and article 49 of the regulation "On the licencing of payment institutions and electronic money institutions and the registration of payment service providers" for electronic money institutions, as well as with the requirements of the Chapter V of the regulation "On the core management principles of banks and branches of foreign banks and the criteria on the approval of their administrators" for banks;
c) the confidentiality of sensitive data and the quality, consistency, integrity and reliability of the information to be provided by the third party to the Bank of Albania, are properly ensured.

3.5.2 Payment service providers wishing to allow the designated third party to fulfil the reporting obligations in a consolidated way (i.e. by presenting one single report referring to several payment service providers affected by the same major operational or security incident), should inform the Bank of Albania, provide the contact information included under "Affected payment service provider" item in the form and ensure the following conditions are satisfied:

a) the payment service provider includes this provision in the contract underpinning the reporting through third parties;
b) the payment service provider makes the consolidated reporting conditional on the incident being caused by a disruption in the services provided by the third party;
c) the payment service provider confines the consolidated reporting to payment service providers established in Albania;

d) the payment service provider provides a list of all payment service providers affected by the incident;
e) the payment service provider ensures that the third party assesses the materiality of the incident for each affected payment service provider and only includes in the consolidated report those payment service providers for which the incident is classified as major, as well as, ensures that, in the event of doubt, if an incident is classified as major for a payment service provider, this payment service provider is included in the consolidated report as long as there is no evidence confirming otherwise;
f) the payment service provider ensures that when there are fields of the form where a common answer is not possible (e.g. sections B2, B4 or C3), the third party fills them out individually for each affected payment service provider, further specifying the identity of each payment service provider the information relates to, or uses the cumulative values as observed or estimated for the payment service providers;
g) the payment service provider ensures that the third party keeps the payment service provider informed at all times of all the relevant information regarding the incident and all the interactions they may have with the Bank of Albania and of the content thereof, but only to the extent possible so as to avoid any breach of confidentiality as regards the information that relates to other payment service providers.

3.5.3 Payment service providers should not transfer to third parties their reporting obligations, before informing the Bank of Albania or after having been notified by the Bank of Albania that the outsourcing agreement does not meet the requirements referred to in letter "b" of the paragraph 3.5.1 of this guideline.

3.5.4 Payment service providers wishing to withdraw the transferring of their reporting obligations to a third party, should immediately communicate this decision to the Bank of Albania. Payment service providers should inform the Bank of Albania of any material development affecting the designated third party for reporting and its ability to fulfil the reporting obligations.

3.5.5 Payment service providers should fulfil their reporting obligations without any support of external assistance whenever the designated third party fails to inform the Bank of Albania of a major operational or security incident in accordance with article 89 of the law "On payment services" and with this guideline. Payment service providers should ensure that an incident is not reported twice, individually by said payment service provider and once again by the designated third party for reporting.

3.5.6 Payment service providers should ensure that, in the situation where an incident is caused by a disruption in the services provided by a technical service provider (or an infrastructure) which affects multiple payment service providers, the delegated reporting refers to the individual data of the payment service provider (except in the case of consolidated reporting).

4. INTERNAL REGULATORY FRAMEWORK OF THE ENTITIES

4.1. The regulatory framework of the entities

4.1.1 Payment service providers should establish an internal regulatory framework, which foresees the incident management procedures, as well as procedures for the detection and classification of major operational and security incidents.

4.1.2 Payment service providers should clearly define in their internal regulatory framework, all responsibilities on incidents reporting, as provisioned in the law "On payment services", as well as the procedures for fulfilling the requirements of this guideline.

CHAIRMAN OF THE SUPERVISORY COUNCIL

Gent SEJKO

ANNEX 1

Initial Report

Major Incident Report					
Initial report	Within 4 hours after classification of the incident as major			Reset dropdown selections	
Report date *(DD/MM/YYYY)*			Time *(HH:MM)*		

A - Initial report						
A 1 - GENERAL DETAILS						
Type of report						
Type of report						
Affected payment service provider (PSP)						
PSP name						
PSP national identification number						
Head of group, if applicable						
Country/countries affected by the incident						
Primary contact person		Email		Telephone		
Secondary contact person		Email		Telephone		
Reporting entity (complete this section if the reporting entity is not the affected PSP in case of reporting through a third party)						
Name of the reporting entity						
National identification number						
Primary contact person		Email		Telephone		
Secondary contact person		Email		Telephone		
A 2 - INCIDENT DETECTION AND CLASSIFICATION						
Date and time of detection of the incident *(DD/MM/YYYY HH:MM)*						
Date and time of classification of the incident *(DD/MM/YYYY HH:MM)*						
The incident was detected by		If 'Other', please specify:				
Type of Incident						
Criteria triggering the major incident report	☐ Transactions affected ☐ Payment service users affected ☐ Service downtime ☐ Breach of security of network or information systems ☐ Economic impact ☐ High level of internal escalation ☐ Other PSPs or relevant infrastructures potentially affected ☐ Reputational impact					
A short and general description of the incident						
Impact in other countries, if applicable						
Reporting to other authorities		If 'Yes', please specify:				
Reasons for late submission of the initial report						

In case the reporting is done on a consolidated basis, please complete the following table:

CONSOLIDATED REPORT - LIST OF PSPs	
PSP Name	**PSP Unique Identification Number**

Intermediate Report

Major Incident Report

Intermediate report — maximum of 3 working days from the submission of the initial report

Reset dropdown selections

Report date *(DD/MM/YYYY)* | Time *(HH:MM)*

B - Intermediate report

B 1 - GENERAL DETAILS

More detailed description of the incident:	
What is the specific issue?	
How did the incident start?	
How did it evolve?	
What are the consequences (in particular for payment service users)?	
Was the incident communicated to payment service users?	If 'Yes', please specify:
Was it related to a previous incident/s?	If 'Yes', please specify:
Were other service providers/third parties affected or involved?	If 'Yes', please specify:
Was crisis management started (internal and/or external)?	If 'Yes', please specify:
Date and time of beginning of the incident (if already identified) *(DD/MM/YYYY HH:MM)*	
Date and time when the incident was restored or is expected to be restored *(DD/MM/YYYY HH:MM)*	
Functional areas affected	☐ Authentication/Authorisation ☐ Direct settlement ☐ Communication ☐ Indirect settlement ☐ Clearing ☐ Other — If 'Other', please specify:
Changes made to previous reports	

B 2 - INCIDENT CLASSIFICATION / INFORMATION ON THE INCIDENT

Transactions affected [2]	Impact level; Number of transactions affected; As a % of regular number of transactions; Value of transactions affected in EUR; Duration of the incident (only applicable to operational incidents); Comments:
Payment service users affected [3]	Impact level; Number of payment service users affected; As a % of total payment service users
Breach of security of network or information systems	Describe how the network or information systems have been affected
Service downtime	Total service downtime: Days: Hours: Minutes:
Economic impact	Impact level; Direct costs in Lek; Indirect costs in Lek
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 PSPs or relevant infrastructures potentially affected	Describe how this incident could affect other PSPs and/or infrastructures
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...)

B 3 - INCIDENT DESCRIPTION

Type of Incident	
Cause of incident	☐ Under investigation ☐ Malicious action ☐ Process failure ☐ System failure ☐ Human errors ☐ External events ☐ Other — If 'Other', please specify:
Was the incident affecting you directly, or indirectly through a service provider?	If 'Indirectly', please provide the service provider's name:

B 4 - INCIDENT IMPACT

Overall impact	☐ Integrity ☐ Availability ☐ Confidentiality ☐ Authenticity
Commercial channels affected	☐ Branches ☐ E-banking ☐ E-commerce ☐ Telephone banking ☐ Mobile banking ☐ ATMs ☐ Point of sale ☐ Other; If 'Other', please specify:
Payment services affected	☐ Cash placement on a payment account ☐ Cash withdrawal from a payment account ☐ Operations required for operating a payment account ☐ Acquiring of payment instruments ☐ Credit transfers ☐ Direct debits ☐ Card payments ☐ Issuing of payment instruments ☐ Money remittance ☐ Payment initiation ☐ Account information services

B 5 - INCIDENT MITIGATION

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? *(DD/MM/YYYY HH:MM)*	
If so, please describe	

Final Report

Major Incident Report

Please select the type of report:

within 20 working days after the submission of the intermediate report

Please describe:
(applicable for incidents reclassified as non-major)

Reset dropdown selections

Report date *(DD/MM/YYYY)* | Time *(HH:MM)*

C - Final report

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

C 1 - GENERAL DETAILS

Update of the information from the initial report and the intermediate report(s)	
Changes made to previous reports	asdfas
Any other relevant information	
Are all original controls in place?	
If "No", specify which controls and the additional period required for their restoration	

C 2 - ROOT CAUSE ANALYSIS AND FOLLOW UP

What was the root cause (if already known)?

☐ Malicious action ☐ Process failure ☐ System failure ☐ Human error ☐ External event ☐ Other

Please specify:

Malicious action	Process failure	System failure	Human error	External event
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
Distributed/Denial of service attack (D/DoS)	Inadequate Change management	Software/application failure	Other	Other
Deliberate internal actions	Inadequacy of internal procedures and documentation	Physical damage		
Deliberate external physical damage	Recovery issues	Other		
Information content security	Other			
Fradulent actions				
Other				

If 'Other', please specify:

Other relevant information on the root cause	
Main corrective actions/measures taken or planned to prevent the incident from happening again in the future, if already known	

C 3 - ADDITIONAL INFORMATON

Has the incident been shared with other PSPs for information purposes?	If 'Yes', please provide details:
Has any legal action been taken against the PSP?	If 'Yes', please provide details:
Assessment of the effectiveness of the action taken	Please provide details:

ANNEX 2

INSTRUCTIONS ON MAJOR INCIDENT REPORTING

Instructions to fill out the reporting templates/forms:

Payment service providers should fill out the relevant section of the form, depending on the reporting phase they are in: section A for the initial report, section B for intermediate reports and section C for the final report. Payment service providers should use the same form when submitting to the Bank of Albania the initial, intermediate and final reports related to the same incident. All fields are mandatory, unless it is clearly specified otherwise in the form.

General information

Initial report: it is the first notification that the PSP submits to the Bank of Albania.

Intermediate report: contains a more detailed description of the incident and its consequences. It is an update of the initial report (and where applicable of a previous intermediate report) on the same incident.

Final report: it is the last report the PSP will send on the incident, since *i)* a root cause analysis has already been carried out and PSP's estimates can be replaced with real figures or *ii)* the incident is no longer considered as major and needs to be reclassified.

Incident reclassified as non-major: the incident no longer fulfils the criteria to be considered as major and is not expected to fulfil them before it is resolved. The PSP should explain the reasons for this reclassification.

Report date and time: exact date and time of submission of the report to the Bank of Albania.

Section A – Initial Report

A1 – General Details

Type of report:

Individual: the report refers to a single PSP.

Consolidated: the report refers to several PSPs within the territory of Republic of Albania that are affected by the same major operational or security incident, which make use of consolidated reporting option. The fields under "Affected PSP" should be left blank (with the exception of the field "Country/Countries affected by the incident") and a list of the PSPs included in the report should be provided by filling in the corresponding table (Consolidated report – List of PSPs).

Affected PSP: refers to the PSP that is experiencing the incident.

PSP name: full name of the PSP subject to the reporting procedure, as it appears in the public register of payment service providers.

PSP national identification number: the licence number isued by the Bank of Albania, as it appears in the public register of payment service providers.

Head of group: in the case of groups of entities as defined in article 5, point 12 of the law "On payment services", the name of the main entity of the group is indicated.

Country/countries affected by the incident: country or countries where the impact of the incident has materialised (e.g. several branches of a PSP located in different countries are affected), irrespective of the severity of the incident in the other countries.

Primary contact person: name and surname of the person responsible for reporting the incident or, in the event that a third party reports on behalf of the affected PSP, name and surname of the person in charge of the incident management/risk department or similar structures at the affected PSP.

Email: email address to which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate email address.

Telephone: telephone number through which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate telephone number.

Secondary contact person: name and surname of an alternative person that could be contacted by the Bank of Albania to inquiry about an incident, when the primary contact person is not available. In the case of a third party reporting on behalf of the affected PSP, name and surname of an alternative person in the incident management/risk department or similar structures at the affected PSP.

Email: email address of the alternative contact person to which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate email address.

Telephone: telephone number of the alternative contact person, through which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate telephone number.

Reporting entity: this section should be completed in the case of a third party fulfilling the reporting obligations on behalf of the affected PSP.

Name of the reporting entity: full name of the entity that reports the incident, as it appears in the National Business Center registry.

National identification number: the unique national identification number used in the country where the third party is located to identify the entity that is reporting the incident. If the reporting third party is a PSP, the national identification number should be the national identification number of the PSP (Licence number) issued by the Bank of Albania.

Primary contact person: name and surname of the person responsible for reporting the incident.

Email: email address to which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate email address.

Telephone: telephone number through which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate telephone number.

Secondary contact person: name and surname of an alternative person in the entity that is reporting the incident that could be contacted by the Bank of Albania when the primary contact person is not available.

Email: email address of the alternative contact person to which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate email address.

Telephone: telephone number of the alternative contact person through which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate telephone number.

A2 - Incident detection and classification

Date and time of detection of the incident: date and time when the incident was first identified.

Date and time of classification of the incident: date and time when the security or operational incident was classified as major.

Incident detected by: indicate whether the incident was detected by a payment service user, by structures within the PSP (e.g. internal audit function) or by another external party (e.g. external service provider). If it was none of those, please provide an explanation in the corresponding field.

Type of incident: indicate whether, to the best of your knowledge and if the information is available, it is an operational or a security incident.

> **Operational incident:** incident stemming from inadequate or failed internal processes and systems, human errors or events of force majeure that affect the integrity, availability, confidentiality and/or authenticity of payment-related services.
>
> **Security incident:** unauthorised access, use, disclosure, disruption, modification or destruction of the PSP's assets that affects the integrity, availability, confidentiality and/or authenticity of payment-related services. This may happen, among other things, when the PSP experiences a breach of security of network or information systems.

Criteria triggering the major incident report: please indicate which of the criteria have triggered the major incident report. Multiple choices may be selected between the criteria: transactions affected; payment service users affected; service downtime; breach of security of network or information systems; economic impact; high level of internal escalation; other PSPs or relevant infrastructures potentially affected; and/or reputational impact.

A short and general description of the incident: please explain briefly the most relevant issues of the incident, covering possible causes, immediate impacts, etc.

Impact in other countries, if applicable: please explain briefly the impact the incident had in other countries (e.g. on payment service users, other PSPs and/or payment infrastructures).

Reporting to other authorities: please indicate whether the incident has been/will be reported to other authorities under separate incident reporting frameworks, if known at the time of reporting. If so, please specify the respective authorities.

Reasons for late submission of the initial report: please explain the reasons why you required longer than 24 hours to classify the incident.

Section B – Intermediate Report

B1 – General Details

More detailed description of the incident: please describe the main features of the incident, covering at least the information on the specific issue and the related background, the description of how the incident started and evolved, and the consequences, especially for payment service users, etc. Please also provide information about the communication with payment service users, if applicable.

Was the incident related to previous incidents? Please indicate whether or not the incident is related to previous incidents, if this information is available. If the incident has been related to previous incidents, please specify which ones.

Were other service providers or third parties affected or involved in the incident? Please indicate whether or not the incident has affected or involved other service providers/third parties, if this information is available. If the incident has affected or involved other service providers/third parties, please list them and provide more information.

Was crisis management started (internal and/or external)? Please indicate whether or not crisis management (internal and/or external) has started. If crisis management has started, please provide more information.

Date and time of beginning of the incident: date and time when the incident started, if known.

Date and time when the incident was restored or is expected to be restored: indicate the date and time when the incident was or is expected to be under control and business was or is expected to be back to normal.

Functional areas affected: indicate the steps of the payment process that have been impacted by the incident, such as authentication/authorisation, communication, clearing, direct settlement, indirect settlement, etc.

> **Authentication/authorization**: procedures which allow the PSP to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials and the payment service user (or a third party acting on behalf of that user) giving their consent in order to transfer funds.
>
> **Communication:** flow of information for the purpose of identification, authentication, notification and information between account servicing payment service providers and payment initiation service providers, account information service providers, payers, payees and other PSPs.
>
> **Clearing:** the process of transmitting, reconciling and, in some cases, confirming transfer orders prior to settlement, potentially including the netting of orders and the establishment of final positions for settlement.

Direct settlement: the completion of a transaction or of processing with the aim of discharging participants' obligations through the transfer of funds, when this action is carried out by the affected PSP itself.

Indirect settlement: the completion of a transaction or of processing with the aim of discharging participants' obligations through the transfer of funds, when this action is carried out by another PSP on behalf of the affected PSP.

Other: the functional area affected is none of the above. Further details should be provided in the free text field.

Changes made to previous reports: please indicate the changes made to the information provided with previous reports related to the same incident (e.g. the initial or, where applicable, an intermediate report).

B2 - Incident classification / Information on the incident

Transactions affected: PSPs should indicate which thresholds are or will likely be reached by the incident, if any, and the related figures: number of transactions affected by the incident, percentage of transactions affected in relation to the number of payment transactions carried out with the same payment services that have been affected by the incident and total value of the transactions. PSPs should provide concrete values for these variables, which may be either actual figures or PSP's own estimates. As a general rule, PSPs should consider as "transactions affected" all domestic and cross-border transactions that have been or will likely be directly or indirectly impacted by the incident and, in particular, those transactions that could not be initiated or processed, those for which the content of the payment message was altered and those that were fraudulently ordered (have the funds been recovered or not). Furthermore, PSPs should consider as the regular level of payment transactions, the daily annual average of domestic and cross-border payment transactions carried out with the same payment services that have been affected by the incident, taking the previous year as the reference period for calculations. If PSPs do not consider this figure to be representative (e.g. due to seasonality), they should use another more representative metric instead and notify to the Bank of Albania the underlying rationale for this approach in the field "Comments".

In the cases where payment transactions in currencies other than local currency Lek are affected by the incident, when calculating the thresholds and reporting the value of the transactions affected, PSPs should convert in Lek the amount of the transactions in another currency, by using the official reference exchange rate published by the Bank of Albania in the day preceding the submission of the incident report.

Payment service users affected by the incident: PSPs should indicate which thresholds are or will likely be reached by the incident, if any, and the related figures: total number of payment service users that have been impacted and percentage of payment service users affected in relation to the total number of payment service users.

PSPs should provide concrete values for these variables, which may be either actual figures or PSP's own estimates. PSPs should consider as "payment service users affected by the incident" all customers (either domestic or from abroad, consumers or corporates) that have a contract with the affected PSP that grants them access to the affected payment service, and that have suffered or will likely suffer the consequences of the incident.

PSPs should use estimates based on their past activity in order to determine the number of payment service users that may have been using the payment service during the lifetime of the incident. In the case of groups, each PSP should only consider their own payment service users. In the case of a PSP offering operational services to others, that PSP should only consider its own payment service users (if any), and the PSPs receiving those operational services should also assess the incident in relation to their own payment service users. Furthermore, PSPs should consider as the total number of payment service users the aggregated figure of domestic and cross-border payment service users contractually bound with them at the time of the incident (or, alternatively, the most recent figure available) and with access to the affected payment service, regardless of their size or whether they are considered active or passive payment service users.

Breach of security of network or information systems: PSPs should determine whether any malicious action has compromised the availability, authenticity, integrity or confidentiality of network or information systems (including data) related to the provision of payment services.

Service downtime: PSPs should indicate whether the threshold is or will likely be reached by the incident and present the related figures: total service downtime. PSPs should provide concrete values for this variable, which may be either actual figures or PSP's own estimates. PSPs should consider the period of time for which any task, process or channel related to the provision of payment services is or will likely be down and thus prevents the initiation and/or execution of a payment service and/or access to a payment account. PSPs should count the service downtime from the moment the downtime starts, and they should consider both the time intervals when they are open for business as required for the execution of payment services and the closing hours and maintenance periods, where relevant and applicable. If payment service providers are unable to determine when the service downtime started, they should exceptionally count the service downtime from the moment the downtime is detected.

Economic impact: PSPs should indicate whether the threshold is or will likely be reached by the incident and present the related figures: direct costs and indirect costs related to the incident. PSPs should provide concrete values for these variables, which may be either actual figures or PSP's own estimates. PSPs should consider both the costs that can be connected to the incident directly and those which are indirectly related to the incident. PSPs should take into account expropriated funds or assets, replacement costs of hardware or software, other legal or remediation costs, fees due to non-compliance with contractual obligations, sanctions, external liabilities and lost revenues. As regards the indirect costs, PSPs should only consider those that are already known or very likely to materialise.

In the cases where costs are in currencies other than local currency Lek, when calculating the threshold and reporting the value of the economic impact, PSPs should convert the amount of the costs in another currency to local currency Lek, by using the official reference

exchange rate published by the Bank of Albania, for the day preceding the submission of the incident report.

Direct costs: costs (in Lek) directly caused by the incident, including costs for the correction of the incident (e.g. expropriated funds or assets, replacement costs of hardware and software, fees due to non-compliance with contractual obligations, etc.).

Indirect costs: costs (in Lek) indirectly caused by the incident (e.g. customer redress/compensation costs, potential legal costs, etc.).

High level of internal escalation: PSPs should consider whether, as a result of the impact on payment-related services, the management body has been or will likely be informed, about the incident outside any periodical notification procedure (ad-hoc) and on a continuous basis throughout the lifetime of the incident. Furthermore, payment service providers should consider whether, as a result of the impact of the incident on payment-related services, a crisis mode has been or is likely to be triggered.

Other PSPs or relevant infrastructures potentially affected by the incident: PSPs should assess the impact of the incident on the financial market, understood as the financial market infrastructures and/or payment schemes that support it and the rest of the PSPs. In particular, PSPs should assess whether the incident has been or will likely be replicated at other PSPs, whether it has affected or will likely affect the smooth functioning of financial market infrastructures or whether it has compromised or will likely compromise the solidity of the financial system as a whole. PSPs should bear in mind various dimensions such as whether the component/software affected is proprietary or generally available, whether the compromised network is internal or external or whether the PSP has stopped or will likely stop fulfilling its obligations in the financial market infrastructures it is a member of (participant).

Reputational impact: PSPs should consider the level of visibility that, to the best of their knowledge, the incident has gained or will likely gain in the marketplace. In particular, PSPs should consider the likelihood of the incident causing harm to society, as a good indicator of its potential to impact their reputation. PSPs should take into account whether:

i. payment service users and/or other PSPs have complained about the adverse impact of the incident;
ii. the incident has impacted a visible payment service related process and is therefore likely to receive or has already received media coverage (considering not only traditional media, such as newspapers, but also blogs, social networks, etc.); media coverage in this context means not only a few negative comments by followers, there should be a valid report or a significant number of negative comments/alerts;
iii. contractual obligations have been or will likely be missed, resulting in the publication of legal actions against the payment service provider;
iv. regulatory requirements have not been complied with, resulting in the imposition of supervisory measures or sanctions that have been or will likely be made publicly available; and
v. a similar type of incident has occurred before.

B3 – Incident description

Type of incident: indicate if the incident is an operational or a security incident. Further explanation is provided in the corresponding field in the initial report.

Cause of incident: indicate the cause of the incident and, if it is not known yet, the one that is the most likely. Multiple choices may be selected from the following alternatives.

Under investigation: please check this alternative, when the cause is currently unknown**.**

Malicious action: are actions intentionally targeting the PSP. These cover malicious code, information gathering, intrusions, distributed/denial of service attack (D/DoS), deliberate internal actions, deliberate external physical damage, information content security, fraudulent actions and others. For more details, please refer to section C2 of this form.

Process failure: the cause of the incident was a poor design or execution of the payment process, the process controls and/or the supporting processes (e.g. process for change/migration, testing, configuration, capacity, monitoring).

System failure: the cause of the incident is associated with a non-adequate design, execution, components, specifications, integration or complexity of the systems, networks, infrastructures and databases that support the payment activity.

Human errors: the incident was caused by the unintentional mistake of a person, be it as part of the payment procedure (e.g. uploading the wrong payments batch file into the payments system) or related to the payment procedure somehow (e.g. the power is accidentally cut off and the payment activity is put on hold).

External events: the cause of the incident is associated with events generally outside the PSP's direct control (e.g. natural disasters, a failure of a technical service provider, etc.).

Other: the cause of the incident is none of the above. Further details should be provided in the free text field and the PSP provides the necessary information.

Was the incident affecting you directly, or indirectly through a service provider? Please indicate whether or not the incident has targeted directly the PSP or affects it indirectly through a third party (if this information is available). In the case of an indirect impact, please provide the name of the service provider(s).

B4 – Incident impact

Overall impact: Please indicate which dimensions have been affected by the operational or security incident. Multiple choices may be selected from the following alternatives.

Integrity: the property of safeguarding the accuracy and completeness of assets (including data).

Availability: the property of payment-related services being fully accessible and usable by payment service users, according to acceptable predefined levels from the PSP.

Confidentiality: the property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Authenticity: the property of a source being what it claims to be.

Commercial channels affected: indicate the channel or channels of interaction with payment service users that have been impacted by the incident. Multiple choices may be selected, from the following alternatives.

Branches: place of business (other than the head office) which is a part of a PSP, has no legal personality and carries out directly some or all of the transactions inherent in the business of a PSP.

E-banking: the use of computers to carry out financial transactions over the Internet.

Telephone banking: the use of telephones to carry out financial transactions.

Mobile banking: the use of a specific banking application on a smartphone or similar device to carry out financial transactions.

ATM: an electromechanical device that allows payment service users to withdraw cash from their accounts and/or access other services (deposits, transfers).

Point of sale: physical premises of the merchant at which the payment transaction is initiated.

E-commerce: the payment transaction is initiated at a virtual point of sale (e.g. for payments initiated via the Internet using credit transfers, payment cards, transfer of electronic money between e-money accounts).

Other: the commercial channel affected is none of the above. Further details should be provided in the free text field and the PSP provides necessary informacion.

Payment services affected: indicate those payment services that are not working properly as a result of the incident. Multiple choices may be selected from the following alternatives.

Cash placement on a payment account: the handing of cash to a PSP in order to credit it on a payment account.

Cash withdrawal from a payment account: the request received by a PSP from its payment service user to provide cash and to debit their payment account by the corresponding amount.

Operations required for operating a payment account: those actions needed to be performed in a payment account in order to activate, deactivate and/or maintain it (e.g. opening, blocking of the account, etc.).

Acquiring of payment instruments: a payment service consisting of a PSP contracting with a payee to accept and process payment transactions, which results in a transfer of funds to the payee.

Credit transfers: a payment service for crediting a payee's payment account with a payment transaction or a series of payment transactions, from a payer's payment account

by the PSP which holds the payer's payment account, based on an instruction given by the payer.

Direct debits: a payment service for debiting a payer's payment account, where a payment transaction is initiated by the payee on the basis of the consent given by the payer to the payee, to the payee's PSP or to the payer's own PSP.

Card payments: a payment service based on a payment card scheme's infrastructure and business rules to make a payment transaction by means of any card, telecommunication, digital or IT device or software, if this results in a debit or a credit card transaction. Card-based payment transactions exclude transactions based on other kinds of payment services.

Issuing of payment instruments: a payment service consisting of a PSP contracting with a payer to provide them with a payment instrument to initiate and process the payer's payment transactions.

Money remittance: a payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another PSP acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee.

Payment initiation services: a payment service to initiate a payment order at the request of the payment service user with respect to a payment account held at another PSP.

Account information services: an online payment service to provide consolidated information on one or more payment accounts held by the payment service user with either another PSP or with more than one PSP.

B5 – Incident mitigation

Which actions/measures have been taken so far or are planned to recover from the incident? Please provide details about actions that have been taken or are planned to be taken in order to temporarily address the incident.

Have the Business Continuity Plan and/or Disaster Recovery Plan been activated? Please indicate whether this plans have been activated, and if so, provide the most relevant details of what happened (e.g. when they were activated and what it consisted of).

Section C – Final Report

C1 – General details

Update of the information from the initial report and the intermediate report(s) (summary): Please provide further information on the incident, including the specific

changes made to the information provided with the intermediate report. Please also include any other relevant information.

Are all original controls in place? Please indicate whether or not the PSP had to cancel or weaken some controls at any time during the incident. If so, please indicate whether all controls are back in place and, if not, explain in the free text field which controls are not back in place and the additional period required for their restoration.

C2 - Root cause analysis and follow up

What was the root cause, if already known? Please indicate what the root cause of the incident is or, if it is not known yet, the one that is the most likely. Multiple choices may be selected from the following alternatives. (Please note that the root cause should be distinguished from the impact of the incident).

Malicious action: external or internal actions intentionally targeting the PSP. These are separated into the following categories:

Malicious code: e.g. a virus, worm, Trojan, spyware, etc.

Information gathering: e.g. scanning, sniffing, social engineering, etc.

Intrusions: e.g. privileged account compromise, unprivileged account compromise, application compromise, bot, etc.

Distributed/Denial of service attack (D/DoS): an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.

Deliberate internal actions: e.g. sabotage, theft.

Deliberate external physical damage: e.g. sabotage, physical attack of the premises/data centres, etc.

Information content security: unauthorised access to information, unauthorised modification of information.

Fraudulent actions: unauthorised use of resources, copyright, masquerade, phishing.

Others (please specify): the cause of the incident is none of the above. Further details should be provided in the free text field and the PSP provides necessary information.

Process failure: the cause of the incident was a poor design or execution of the payment process, the supporting processes controls (e.g. process for change/migration, testing, configuration, capacity, monitoring). These are separated into the following categories:

Deficient monitoring and control: e.g. in relation to running operations, certificate expiry dates, licence expiry dates, patch expiry dates, defined maximum counter values, database fill levels, user rights management, dual control principle, etc.

Communication issues: e.g. between market participants or within the organisation.

Improper operations: e.g. no exchange of certificates, cache is full, etc.

Inadequate change management: e.g. unidentified configuration errors, roll-out including updates, maintenance issues, unexpected errors, etc.

Inadequacy of internal procedures and documentation: e.g. lack of transparency regarding functionalities, processes and occurrence of malfunctioning, absence of documentation, etc.

Recovery issues: e.g. contingency management, inadequate redundancy, etc.

Others (please specify): the cause of the incident is none of the above. Further details should be provided in the free text field and the PSP provides the necessary information.

System failure: the cause of the incident is associated with a non-adequate design, execution, components, specifications, integration or complexity of the systems, networks, infrastructures and databases that support the payment activity. These are separated into the following categories:

Hardware failure: failure of physical technology equipment that runs the processes and/or stores the data needed by PSPs to carry out their payment-related activity (e.g. failure of hard drives, data centres, other infrastructure, etc).

Network failure: failure of telecommunications networks, either public or private, that allow the exchange of data and information (e.g. via the Internet) during the payment process.

Database issues: data structure which stores personal and payment-related information needed to execute payment transactions.

Software/application failure: failures of programs, operating systems, etc. that support the provision of payment services by the PSP (e.g. malfunctions, unknown functions).

Physical damage: e.g. unintentional damage caused by inadequate conditions, construction work, etc.

Other (please specify): the cause of the incident is none of the above. Further details should be provided in the free text field and the PSP provides the necessary information.

Human error: the incident was caused by the unintentional mistake of a person, be it as part of the payment procedure (e.g. uploading the wrong payments batch file into the payments system) or related to the payment procedure somehow (e.g. the power is accidentally cut off and the payment activity is put on hold). These are separated into the following categories:

Unintended: e.g. mistakes, errors, omissions, lack of experience and knowledge.

Inaction: e.g. due to lack of skills, knowledge, experience, awareness, etc.

Insufficient resources: e.g. lack of human resources, availability of staff, etc.

Other (please specify): the cause of the incident is none of the above. Further details should be provided in the free text field and the PSP provides the necessary information.

External event: the cause is associated with events generally outside the organisation's control. These are separated into the following categories:

Failure of a supplier/technical service provider: e.g. power outage, Internet outage, legal issues, business issues, service dependencies, etc.

Force majeure: e.g. power failure, fires, natural causes such as earthquakes, floods, heavy precipitation, heavy wind, etc.

Other (please specify): the cause of the incident is none of the above. Further details should be provided in the free text field and the PSP provides the necessary information.

Other (please specify): the cause of the incident is none of the above. Further details should be provided in the free text field and the PSP provides the necessary information.

Other relevant information on the root cause: Please provide any additional details on the root cause, including the preliminary conclusions drawn from the root cause analysis.

Main corrective actions/measures taken or planned to prevent the incident from happening again in the future, if already known: Please describe the main actions that have been taken or are planned to be taken, in order to prevent a future reoccurrence of the incident.

C3 – Additional Information

Has the incident been shared with other PSPs for information purposes? Please provide an overview as which PSPs have been notified, either formally or informally, about the incident, providing details of the PSPs that have been informed on the incident, the information that has been shared and the underlying reasons for sharing this information.

Has any legal action been taken against the PSP? Please indicate whether, at the time of filling out the final report, the PSP has suffered any legal action (e.g. taken to court, lost its licence) as a result of the incident.

Assessment of the effectiveness of the actions taken: please include, where available, a self-assessment of the effectiveness of the actions taken during the duration of the incident, including any lessons learnt from the incident.