Pursuant to Article 44 paragraph 2 item 3 of the Central Bank of Montenegro Law (OGM 40/10, 06/13, 70/17), and Article 56b paragraph 4 and of the Payment System Law (OGM 62/13/, 111/22), the Council of the Central Bank of Montenegro, at its meeting held on 5 October 2023, passed the following

DECISION
ON REPORTING ON MAJOR INCIDENTS RELATED TO THE PROVISION OF PAYMENT SERVICES

I. BASIC PROVISIONS

Subject matter

Article 1

This Decision shall determine the criteria based on which the providers of payment services classify major operational or security incidents in relation to the provision of payment services, the manner how those incidents are reported to the Central Bank of Montenegro hereinafter: the Central Bank), the criteria based on which the Central Bank estimates the significance of incidents and details from incidents reports that they share with competent authorities.

Application

Article 2

(1) This Decision shall apply to major operational or security incidents, including external and internal events that could either be malicious or accidental.

(2) This Decision shall apply also to major operational or security incidents that originate outside Montenegro, such as incidents that originate in the parent or subsidiary undertaking of the payment services provider, with head office outside Montenegro, and which affect the payment services provided by a payment services provider, either:

1) directly, when a payment-related service is carried out by an undertaking affected by the incident, with head office outside Montenegro; or
2) indirectly, when the capacity of the payment service provider to keep carrying out its payment service is jeopardised in another way as a result of the incident.

(3) This Decision shall apply also to major operational or security incidents affecting activities supported by payment service providers, including activities outsourced by the payment services providers to third parties.

Definitions

Article 3

The terms used in this Decision shall have the following meanings:

1) **operational or security incident** means 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;
2) **integrity** means the property of safeguarding the accuracy and completeness of assets, including data;
3) **availability** means the property of payment services and payment-related services being fully accessible and usable by payment service users, according to acceptable levels predefined by the payment service provider;
4) **confidentiality** means the property that information is not made available or disclosed to unauthorised individuals, entities or processes;
5) **authenticity** means the property of a source (person, process, system, etc.) being what it claims to be.
6) **reestablishment of regular operations** means recovery of regular activities, or operations of a payment service provider following an operational or security incident, up to the service level that existed prior to the incident, and which was internally established by the payment service provider with a third party via a Service Level Agreement, when the contingency measures are no longer applied.
7) **consolidated reporting** means a manner of reporting where a third party prepares one report for several payment service providers impacted by the same major operational or security incidents.

II CLASSIFICATION AND NOTIFICATION

Classification of operational or security incident

Article 4

(1) Payment service provider shall classify as major those operational or security incidents that, the assessment referred to in Article 6 of this Decision, establishes that they fulfil:
1) one or more criteria at the higher impact level; or
2) three or more criteria at the lower impact level.

(2) The criteria of higher and lower impact level referred to in paragraph 1 are given in Annex 1, enclosed with this Decision and making an integral part thereof.

(3) Payment service provider shall perform classification referred to in paragraph 1 of this Article in a timely manner, and not later than 24 hours after the detection of the incident, without undue delay after the information required for the classification of the incident becomes available.

(4) Notwithstanding paragraph 3 of this Article, if the payment service provider requires more than 24 hours to classify a certain incident after its detection, it shall submit to

the Central Bank an initial report of that incident in accordance with the provisions of Article 8 of this Decision.

Criteria for the assessment of operational or security incident

Article 5

Payment service provider shall implement assessments of operational or security incidents based on the following criteria and their core indicators:

1) **Transactions affected -** payment service providers shall determine the total value of the transactions affected, as well as the number of payments compromised as a percentage of the regular level of payment transactions carried out with the affected payment services;
2) **payment service users affected -** payment service providers shall determine the number of payment service users affected both in absolute terms and as a percentage of the total number of payment service users;
3) **breach of security of network or information systems -** payment service providers shall determine whether any malicious action has compromised the security of network or information systems related to the provision of payment services;
4) **service downtime** - payment service providers shall determine the period of time during which the service will likely be unavailable for the payment service user or during which the payment order cannot be fulfilled by the payment service provider;
5) **economic impact** - payment service providers shall 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 (i.e. to the payment service provider's Tier-1 capital);
6) **high level of internal escalation** - payment service providers shall determine whether this incident has been or will likely be reported to members of its management bodies;
7) **other payment service providers or relevant infrastructures potentially affected** - payment service providers shall 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;
8) **reputational impact** - payment service providers shall 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.

Assessment of operational or security incident

Article 6

(1) Payment service provider shall perform an assessment of operational or security incident by determining, for each individual criterion referred to in Article 5 of this

Decision, whether the thresholds in Annex 1 of this Decision are or will likely be reached before the incident is solved.

(2) Aimed at performing estimation referred to in paragraph 1 of this Article, payment system provider shall determine the value of the indicator referred to in Article 5 of this Decision, in line with the instruction given in Annex 2 enclosed with this Decision and making an integral part thereof.

(3) In case the payment service provider does not have actual date to support its judgement as to whether a given threshold referred to in paragraph 1 of this Article is or will likely be reached before the operational or security incident is solved, the estimation may be determined based on the estimated data, especially during the initial investigation phase.

(4) Payment service provider shall carry out the assessment referred to in paragraph 1 of this Article on a continuous basis during the lifetime of the operational or security incident, so as to identify any possible status change, with respect to its significance.

(5) Payment service provider shall notify the Central Bank without delay, in line with the provisions of Article 10 paragraphs 7, 8 and 9 of this Decision, on each reclassification of operational or security incident from major to non-major.

Notification of the Central Bank

Article 7

(1) Payment service providers shall collect all relevant information, prepare reports on major operational or security incidents by completing an electronic template given in Annex 3 enclosed with this Decision and making an integral part thereof and submit it to the Central Bank in electronic form.

(2) Payment service providers shall complete all fields of the template referred to in paragraph 1 of this Article.

(3) Payment service providers shall use the same electronic template referred to in paragraph (1) of this Article when submitting the initial, intermediate and final reports related to the same operational or security incident, that is payment service providers shall complete a single template in an incremental manner and update, where applicable, the information provided with previously submitted reports.

(4) If the incident referred to in paragraph 1 of this Article impacts or could impact financial interests of payment services users, payment service provider shall provide, without delay, the Central Bank with the copy of an incident notification which was submitted to payment service users, in accordance with the Payment System Law.

(5) Payment service provider shall provide the Central Bank, at the request, without delay, with additional documentation complementing the information submitted in reports referred to in paragraph 1 of this Article and clarifications in relation to the already submitted documentation.

(6) Payment service provider shall, in the template referred to in paragraph 1 of this Article, indicate any additional information contained in documentation submitted to the Central Bank, either on the initiative of the payment service provider or upon the request of the Central Bank in line with paragraph 5 of this Article.

(7) Payment service provider shall at all times preserve confidentiality and integrity of the information exchanged with the Central Bank and appropriately confirm its identity to the Central Bank.

(8) The Central Bank shall publish electronic template referred to in paragraph 1 of this Article on its web page as well as the manual on how to fill out that template.

Initial report

Article 8

(1) Payment service provider shall submit an initial report on operational or security incident to the Central Bank:

1) not later than four hours after the incident has been classified as major;
2) not later than 24 hours after the detection of the incident, if the payment service provider requires more than 24 hours to classify the incident from the moment it was detected;
3) immediately after the incident which was not classified as major became reclassified as major.

(2) Payment service provider shall create the initial report referred to in paragraph 1 of this Article by filling out fields in the section “A” of the template referred to in Article 7 paragraph 1 of this Decision, by stating basic characteristics of the incident and its foreseen consequences based on the available information.

(3) If the payment service provider does not have all actual data on the incident at the moment the initial report referred to in paragraph 1 of this Article is created, it should resort to estimation.

(4) If the payment service provider requires more than 24 hours to classify the incident from the moment of its detection, it shall state reasons for that in the initial report referred to in paragraph 1 of this Article.

(5) Notwithstanding paragraph 1 of this Article, if the payment service provider is not able to submit the initial report within the envisaged deadline because the reporting channels of the Central bank are not available or functional, it shall submit the initial report as soon as the channels become available and/or functional.

(6) After receiving the initial report referred to in paragraph 1 of this Article, the Central Bank shall without delay, confirm the receipt of the report to the payment service provider and allocate unique identification number of the incident and inform the payment service provider thereof.

(7) Payment service provider shall state the unique identification number of the incident referred to in paragraph 6 of this Article in all subsequent reports on this

incident, that is in the updated initial report or intermediate and final report on this incident, if it failed to submit it with the initial report.

Intermediate report

Article 9

(1) Payment service provider shall submit the intermediate report on operational or security incident to the Central Bank:

1) immediately after the regular activities have been recovered and payment service provider's business is back to normal;
2) within three working days from the submission of the initial report, if payment service provider's regular activities have not yet been recovered.

(2) Payment service provider shall create intermediate report referred to in paragraph 1 of this Article by filling out fields in the section "B" of the template referred to in Article 7 paragraph 1 of this Decision, by giving a detailed description of the incident and its consequences.

(3) Payment service provider shall update information provided in sections "A" and "B" of the template referred to in Article 7 paragraph 1 of this Decision and submit them to the Central Bank without delay:

1) after submitting previous reports to the Central Bank, when there are significant changes in relation to operational or security incident, including detection of additional causes of that incited or additional actions taken to fix the problem;
2) when the operational or security incident has not been resolved within three working days from the moment it was detected;
3) at the request of the Central Bank.

(4) If the payment service provider does not have all actual data on the operational or security incident at the moment the report referred to in paragraphs 1 and 3 of this Article is created, it should resort to estimation.

(5) Should business be back to normal before four hours have passed since the operational or security incident was classified as major, payment service providers should aim at simultaneously submitting both the initial and the intermediate report within the four-hour deadline.

Final report

Article 10

(1) Payment service provider shall submit a final report on major operational or security incidents to the Central Bank after it performs the root cause analysis, regardless of whether risk and consequences mitigation measures have already been implemented or the final root cause of operational or security incident has been identified, and when there are actual figures available to replace any data obtained based on the estimates referred to in Article 8 paragraph 3 and Article 9 paragraph 4 of this Decision.

(2) Payment service providers shall submit the final report referred to in paragraph 1 of this Article to the Central Bank in a maximum of 20 working days after payment service provider's business is deemed back to normal.

(3) Notwithstanding paragraph 2 of this Article, payment service provider needing an extension of the deadline for the submission of the final report shall provide the Central Bank, before the time has elapsed, a request for the postponement of the submission of the final report with detailed clarification of the reasons for the postponement as well as a new deadline for its submission.

(4) Payment service provider shall create the final report referred to in paragraph 1 of this Article by filling out the section "C" of the template referred to in paragraph 1 of this Decision, by stating the information on root cause of operational or security incident, if the root cause is known, and the information on taken or planned measures for the removal of the problem and preventing its reoccurrence in the future.

(5) Payment service providers shall compose the final report referred to in paragraph 1 of this Article based on actual data, and use those data to update information previously submitted in sections "A" and "B" of the templates referred to in Article 7 paragraph 1 of this Decision.

(6) If the payment service provider is able to provide the Central Bank with all the information from section "C" of the template referred to in Article 7 paragraph 1 of this Decision within the four-hour window since the incident was classified as major, it shall provide the Central Bank with the initial, intermediate, and final reports together.

(7) Payment service provider shall submit the Central Bank with final report on operational or security incident when, as a result of continuous assessment of the incident referred to in Article 6 paragraph 4 of this Decision it identifies that an already reported incident no longer fulfils the criteria to be considered major and that is does not expect to fulfil them before the incident is resolved.

(8) In the case referred to in paragraph 7 of this Article, the payment service provider shall submit the final report to the Central Bank as soon as possible, following the reclassification of the incident, within the deadline for the submission of the next report.

(9) When composing the final report referred to in paragraph 7 of this Article, the payment service provider shall not fill out the entire section "C" of the template referred to in Article 7 paragraph 1 of this Decision, but the payment service provider shall check the box "incident reclassified as non-major" and state the reasons justifying this reclassification.

Delegated and consolidated reporting

Article 11

(1) Reporting on major operational or security incidents that the payment service provider, in accordance with the law, delegates to a third party shall be performed in a manner specified by this Decision.

(2) Payment service provider may, by way of contract on the outsourcing of certain operational activities to a third party, delegate reporting in line with this decision and consolidated reporting on incidents caused by disruption in the services provided by the third party, provided that:

1) before submitting consolidated incidents reports, it duly informed the Central Bank on that delegation and provide the contract information from the section of the template referred to in Article 7 paragraph 1 of this Decision under “Affected payment service provider (PSP)”;
2) the provision on consolidated reporting is clearly stated in the contract on delegation of operational activities;
3) consolidated reporting refers only on the incidents caused by a disruption in the services provided by the third party;
4) consolidated reporting refers only to payment service providers having their head offices in Montenegro;
5) consolidated report is supplemented by a list of all payment service providers affected by the incident;
6) the third party assesses the materiality of the operational or security incident for each affected payment service provider and only includes in the consolidated report those payment service providers for which the operational or security incident is classified as major;
7) in the event of doubt regarding the materiality of operational or security incident for a certain payment service provider, that payment service provider is included in the consolidated report as long as there is no evidence confirming the materiality of that incident;
8) in case when there are fields of the template where a common answer for all payment service providers is not possible (e.g. sections B2, B4 or C3 of the template referred to in Article 7 paragraph 1 of this Decision), the sections are filled 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 affected payment service providers;
9) 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 Central Bank, to the extent possible so as to avoid any breach of confidentiality as regards the information that relates to other payment service providers.

(4) Payment service providers wishing to withdraw the delegation of their reporting obligations in line with paragraphs 1 and 2 of this Article, shall without delay communicate this decision to the Central Bank.

(5) Payment service provider shall without delay inform the Central Bank of any material development affecting the third party to which it delegated the reporting in line with paragraphs 1 and 2 of this Article and its ability to fulfil the reporting obligations.

(6) Payment service provider shall inform the Central Bank on major operational or security incidents in line with the provision of this Decision, if the third person to which it delegated the reporting fails to inform the Central Bank.

(7) Payment service provider shall ensure that the reporting in line with this Article is performed in a manner which avoids reporting on the same incident by several persons.

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

III. INTERNAL ACTS

Procedures for reporting on operational or security incidents

Article 12

Payment service provider shall establish a procedure for reporting on operational or security incidents which contains clearly described roles and responsibilities for reporting on those incidents as well as detailed description of procedures that the payment service provider established for the purpose of acting in accordance with the provisions of this Decision.

IV. EXCHANGE OF INFORMATION WITH OTHER COMPETENT AUTHORITIES

Assessment of materiality of the incident to other competent authorities

Article 13

(1) The Central Bank shall assess the relevance of the reported major operational or security incidents to other competent authorities, taking into account the following criteria, or whether:

1) the causes of the incident are within the remit of another authority;
2) the consequences of the incident have an impact on the legally prescribed objectives of another domestic authority;
3) the incident affects, or could affect, payment service users on a wide scale;
4) the incident is likely to receive, or has received, wide media coverage.

(2) The Central Bank shall carry out assessment referred to in paragraph 1 of this Article on a continuous basis during the lifetime of the operational or security incident, so as to identify any possible change that could make relevant an incident to another competent authority.

Incident information to be shared with other competent authorities

Article 14

(1) The Central Bank shall provide information about major operational or security incidents to other competent authority immediately after receiving the initial report or

other report based on which it assessed it to be relevant for that authority and immediately after receiving information that the business of the affected payment service provider is back to normal, or after receiving the intermediate report.

(2) Aimed at providing a clear picture about the operational or security incident and its possible consequences, the Central Bank shall provide the following information from the intermediate report or intermediate report on the incident to another competent authority, while taking care of the confidentiality and integrity of data:

1) date and time of classification of the incident as major;
2) date and time of detection of the incident;
3) date and time of beginning of the incident;
4) date and time when the incident was restored or is expected to be restored;
5) short description of the incident, including non-sensitive parts of the detailed description;
6) short description of measures taken or planned to be taken to recover from the incident;
7) description of how the incident could affect other payment service providers and/or infrastructure;
8) description of media coverage, if any;
9) cause of the incident.

(3) the Central Bank shall conduct anonymisation of data and leave out confidential information and any information subject to intellectual property, before sharing information to another competent authority, unless otherwise prescribed by the law.

(4) Notwithstanding paragraph 3 of this Article, the Central Bank may provide the other competent authority with information on the name and address of incident affected payment service providers, provided that their confidentiality is guaranteed.

V. FINAL PROVISION

Entry into force

Article 15

This Decision shall be published in the “Official Gazette of Montenegro” and it shall come into force on the day of entry into force of the Law amending the Payment System Law (OGM 111/22).

THE COUNCIL OF THE CENTRAL BANK OF MONTENEGRO

CHAIRMAN

Decision number: 0101-7425-2/2023 **G O V**
E R N O R,
Podgorica, 5 October 2023 **Radoje Žugić, m.p.**

ANNEX 1

Criteria	Lower impact level	Higher impact level
Transaction affected by operational or security 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* **or** > EUR 500,000 and duration of the incident > 1 hour*	> 25% of the payment service provider's regular level of transactions (in terms of number of transactions) **or** > EUR 15,000,000
Payment service users affected by operational or security incident	> EUR 5,000 and duration of the incident > 1 hour* **or** 10% of the payment service provider's payment service users and duration of the incident > 1 hour*	> 50,000 **or** > 25% of the payment service provider's payment service users
Service downtime	> two hours	Not applicable
Breach of security of network or information systems	Yes	Not applicable
Economic impact	Not applicable	> Max (0.1% Tier-1 capital**, EUR 200,000) **or** > EUR 5,000,000
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 operational or security incident	Yes	Not applicable
Reputational impact	Yes	Not applicable

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.
**Tier-1 capital in line with regulation of the Central bank governing the manner of calculating the Tier-1 capital of credit institutions, or payment institutions and electronic money institutions.

ANNEX 2

Guideline for determining the value of criteria indicators based on which the assessment of the materiality of the operational or security incident is performed

1. Transactions affected

Transactions affected by operational or security incident shall be all payment 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 shall report only those incidents with a duration longer than one hour. The duration of the incident shall 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.

Regular scope of transactions shall be the daily annual average of payment transactions carried out by the payment services that have been affected by the incident, during the previous year. In case the payment service provider does not consider this figure to be representative (e.g. due to seasonality), they should use a more representative metric instead and provide a detailed rationale for this approach in the corresponding field of the template referred to in Article 7 paragraph 1 of this Decision.

2. Payment service users affected

Payment service users affected by operational or security incident shall be all customers (either domestic or from abroad, natural persons or legal persons) 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. In case of estimation of the number of users of payment services that may have used the payment service during the operational or security incident, such estimation shall be carried out based on past activity of the user of payment service.

Payment service provider that is part of a group shall only consider its own payment service users. Payment service provider offering operational services to other payment service providers shall only consider its own payment service users (if any), and the payment service providers receiving those operational services shall assess the incident in relation to their own payment service users.

In the case of operational incidents affecting the ability to initiate and/or process transactions, payment service providers should report only those incidents that affect

the payment service user longer than one hour, while the duration of the incident shall 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.

The total number of payment service users shall be the determined, or the most recent available number of payment service users with whom the payment service provider was contractually bound at the time of the of the operational or security incident, and with access to the affected payment service. When determining the users of payment services with access to the payment service affected by the operational or security incident, all users shall be taken into consideration, regardless of their size or whether they are considered active or passive payment service users.

3. Breach of security of network or information systems

Payment service providers shall 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.

4. Service downtime

Payment service providers shall consider 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, prevent:

1) the initiation and/or execution of a payment service; and/or
2) access to a payment account.

Payment service providers shall count the service downtime from the moment the downtime starts, while taking into account 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 can exceptionally count the service downtime from the moment the downtime is detected.

5. Economic impact

Payment service providers shall consider both the costs that can be connected to the incident directly and those which are indirectly related to the incident, if those costs are known or are likely to materialise. Payment service providers shall in particular take into account expropriated funds or assets, replacement costs of hardware or software, other forensic or remediation costs, fees due to non-compliance with contractual obligations, sanctions, external liabilities and lost revenues.

6. High level of internal escalation

Payment service providers shall consider whether, as a result of the impact of operational or security incident on payment services and/or payment-related services, its management body has been or will likely be informed on the incident, in line with Article 25 paragraph 3 item 5 indent 2 of the Decision on security measures for operational and security risks related to payment services (OGM 47/23), through

extraordinary reports and on a continuous basis throughout the lifetime of the incident, irrespective of the established periodic reporting procedure. Furthermore, payment service providers shall consider whether, as a result of the impact of the operational or security incident on payment services and/or payment-related services, a crisis mode has been or is likely to be triggered.

7. 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. Payment service providers shall in particular 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. When performing assessment, the payment service providers shall bear in mind various dimensions of the impact of operational or security incident (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).

8. Reputational impact

The payment service provider shall consider the level of visibility that, to the best of their knowledge, the operational or security incident has gained or will likely gain in the marketplace. In particular, the payment service provider shall consider the likelihood of the incident causing harm to community and society as a good indicator of its potential to impact their reputation.

The payment service provider shall take into account whether:

1) payment service users and/or other payment service providers have complained about the adverse impact of the incident;
2) 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.);
3) contractual obligations have been or will likely be breached, resulting in the publication of legal actions against the payment service provider;
4) 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;
5) a similar type of incident has occurred before.