Instruction No. 4

Measures for Management of Operational and Security Risks Related to Payment Services and Connected Reporting Duties

THE FINANCIAL INFORMATION AUTHORITY

Having regard to Article 61 (1) of Regulation No. 3 *on payment services provided by entities carrying out financial activities on a professional basis* of 23 May 2018 ("Regulation No. 3"), according to which payment service providers shall establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks, relating to the payment services they provide;

Having regard to Article 61 (2) of Regulation No. 3, according to which payment service providers shall provide to the Financial Information Authority an updated and comprehensive assessment of the operational and security risks relating to the payment services they provide and on the adequacy of the mitigation measures and control mechanisms implemented in response to those risks;

Having regard to Article 61 (3) of Regulation No. 3, according to which the Financial Information Authority issues guidelines and regulatory technical standards on the classification of major operational and security incidents, as well as on the criteria and conditions for establishment, and monitoring, of security measures;

Having regard to Article 62 (1) of Regulation No. 3, according to which in case of a major operational or security incident, payment service providers shall notify the Financial Information Authority;

Having regard to Article 62 (2) of Regulation No. 3, according to which the Financial Information Authority issues guidelines and regulatory technical standards on the reporting of major operational or security incidents;

Taking into account the guidelines adopted by relevant international and European bodies on the matter;

Giving execution to the resolution adopted by the Board of Directors on 5 April 2018;

PROMULGATES THE FOLLOWING INSTRUCTION

Title I

Scope of Application, Object and Definitions

Article 1. *Scope of Application*

This Instruction applies to entities carrying out financial activities on a professional basis within the State, authorized for issuing and managing means of payment ("payment service providers") and within the scope of application of Regulation No. 3 of 23 May 2018 ("Regulation No. 3").

Article 2. *Object*

1. This Instruction is about:

a) Requirements for the establishment, implementation and monitoring of the security measures that payment service providers must take, in accordance with Article 61 (1) of Regulation No. 3, to manage the operational and security risks relating to the payment services they provide;

b) The criteria for the classification of major operational or security incidents by payment service providers, as well as the format and procedures they shall follow to notify such incidents to the Financial Information Authority, as laid down in Article 62 (1) of Regulation No. 3.

Article 3. *Definitions*

1. For the purposes of this Instruction, the same definitions as under Article 3 of Regulation No. 1 of 25 September 2014, and Article 4 of Regulation No. 3 apply, as well as the following definitions:

2. «*Authenticity*»: the property of a source being what it claims to be.

3. «*Continuity*»: the property of an organization's processes, tasks and assets needed for the delivery of payment-related services being fully accessible and running at acceptable pre-defined levels.

4. «*Defence in-depth*»: the implementation of more than one control covering the same risk, such as the four-eyes principle, two-factor authentication, network segmentation and multiple firewalls.

5. «*Availability*»: the property of payment-related services being accessible and usable by payment service users.

6. «*Operational or security incident*»: a singular event or a series of linked events unplanned by the payment service provider which has or will probably have an adverse impact on the integrity, availability, confidentiality, authenticity and/or continuity of payment-related services.

7. «*Integrity*»: the property of safeguarding the accuracy and completeness of assets (including data).

8. «*Risk appetite*»: aggregate level and types of risk an entity is willing to assume within its risk capacity, in line with its activity model, to achieve its strategic objectives.

9. «*Security risk*»: the risk resulting from inadequate or failed internal processes or external events that have or may have an adverse impact on the availability, integrity, confidentiality of information and communication technology (ICT) systems and/or information used for the provision of payment services. This includes risk from cyber-attacks or inadequate physical security.

10. «*Confidentiality*»: the property according to which information is not made available or disclosed to unauthorized individuals or entities.

11. « *Payment-related services*»: Any ancillary activity and all the necessary technical supporting tasks for the correct provision of payment services.

Title II

Security Measures to Manage Operational and Security Risks

Article 4. *General Principles*

1. Payment service providers shall comply with the provisions set out in this Title consistently with the criteria of application established by Article 3 of Regulation No. 3.

2. In particular, all provisions shall be applied consistently with the principle of proportionality, by taking into account the payment service provider's size and the nature, scope, complexity and riskiness of the particular services that the payment service provider provides or intends to provide.

Chapter 1

Principles of Good Governance and Organization

Article 5. *Reference Framework for Operational and Security Risk Management*

1. Payment service providers shall establish an effective operational and security risk management framework ('reference framework').

2. This framework shall have as its object the security measures to mitigate operational and security risks and it shall be fully integrated into the payment service provider's overall risk management processes.

In particular, the framework shall:

a) Include a comprehensive security policy document, including a detailed risk assessment in relation to its payment services and a description of security control and mitigation measures taken to adequately protect payment service users against the risks identified, including fraud and illegal use of sensitive and personal data;

b) Be consistent with the risk appetite of the payment service provider;

c) Define and assign key roles and responsibilities as well as the relevant reporting lines required to enforce the security measures and to manage security and operational risks;

d) Establish the necessary procedures and systems to identify, measure, monitor and manage the range of risks stemming from the payment-related activities of the payment service provider and to which the payment service provider is exposed, including business continuity arrangements.

3. Payment service providers shall ensure that the framework is properly documented, and updated with documented 'lessons learned' during its implementation and monitoring.

4. Payment service providers shall ensure that before a major change of infrastructure, processes or procedures, and after each major operational or security incident affecting the security of the payment services they provide, they review whether or not changes or improvements to the risk management framework are needed without undue delay.

5. The framework shall be developed and updated, once a year, by the risk management function, approved by the management and adopted by the senior management.

6. Payment service providers shall communicate the framework referred to in this Article, within 30 days of the adoption or the annual update, to the Financial Information Authority, which may require its review.

Article 6. *Risk Management and Control Models*

1. Payment service providers shall establish three effective lines of defence, or an equivalent internal risk management and control model, to identify and manage operational and security risks.

2. The internal control model shall be developed and updated, once a year, by the risk management function, approved by the management and adopted by the senior management.

3. Payment service providers shall ensure that the internal control model adopted has sufficient authority, independence, resources and direct reporting lines to the management and, where relevant, to the senior management.

4. The internal control model adopted, including the security measures set out, shall be audited by external auditors with expertise in IT security and payments and operationally independent within or from the payment service provider.

The frequency and focus of such audits shall take the corresponding security risks into consideration.

5. Payment service providers shall communicate the internal control model adopted and the reports by external auditors to the Financial Information Authority, within 30 days of the adoption or the annual update.

Chapter 2

Risk Assessment

Article 7. *Identification of Functions, Processes and Assets*

1. Payment service providers shall identify, establish and regularly update an inventory of their internal functions and offices, key roles and supporting processes in order to map the importance of each function, office, role and supporting process, and their interdependencies related to operational and security risks.

2. Payment service providers shall identify, establish and regularly update an inventory of the information assets, such as ICT systems, their configurations, other infrastructures, and also the interconnections with other internal and external systems in order to be able to manage the assets that support their critical internal functions, offices and processes.

Article 8. *Classification of functions, Processes and Assets*

Payment service providers shall classify the identified internal functions and offices, supporting processes, and information assets in terms of criticality.

Article 9. *Risk Assessment of Functions, Processes and Assets*

1. Payment service providers shall ensure that they continuously monitor threats and vulnerabilities, and regularly review the risk scenarios impacting their internal functions and offices, critical processes and information assets.

2. Payment service providers shall carry out and document risk assessment, once a year, of the internal functions and offices, processes and information assets they have identified and classified in order to identify and assess key operational and security risks. Such risk assessment shall also be carried out before any major change of infrastructure, process or procedures affecting the security of payment services occurs.

3. On the basis of the risk assessment of the operational and security risks relating to the payment services they provide, payment service providers shall determine whether and to what extent changes are necessary to the existing security measures, the technologies used and the procedures or payment services offered.

Payment service providers shall take into account the time required to implement the changes and the time to take appropriate interim security measures to minimize operational or security incidents, fraud and potential disruptive effects in the provision of payment services.

4. The risk assessment of the operational and security risks relating to the payment services, including the mitigating measures and control mechanisms implemented in response to those risks, shall be carried out and updated by the risk management function, approved by the management and adopted by the senior management.

5. Payment service providers shall provide Financial Information Authority, within 30 days of the adoption or the annual update, with an updated and comprehensive risk assessment of the operational and security risks relating to the payment services they provide and on the adequacy of the mitigating measures and control mechanisms implemented in response to those risks.

Chapter 3

Protection

Article 10. *Preventive Security Measures*

1. Payment service providers shall establish and implement preventive security measures against identified operational and security risks. These measures shall ensure an adequate level of security in accordance with the risks identified.

2. Payment service providers shall establish and implement a 'defence-in-depth' approach by instituting multi-layered controls covering people, processes and technology, with each layer serving as a safety net for preceding layers.

3. Payment service providers shall ensure the confidentiality, integrity and availability of their critical logical and physical assets, resources and sensitive payment data of their users whether at rest, in transit or in use.

4. On an on-going basis, payment service providers shall determine whether changes in the existing operational environment influence the existing security measures or require the adoption of further measures to mitigate the risk involved.

These changes should be part of the payment service provider's formal change management process, which should ensure that changes are properly planned, tested, documented and authorized.

On the basis of the security threats observed and the changes made, testing shall be performed to incorporate scenarios of relevant and known potential attacks.

5. In designing, developing and providing payment services, payment service providers shall ensure that segregation of duties and 'least privilege' principles are applied.

Payment service providers shall pay special attention to the segregation of IT environments, in particular to the development, testing and production environments.

Article 11. *Data and Systems Integrity and Confidentiality*

1. In designing, developing and providing payment services, payment service providers shall ensure that the collection, routing, processing, storing and/or archiving and visualization of sensitive payment data of the users is adequate, relevant and limited to what is necessary for the provision of its payment services.

2. Payment service providers shall regularly check that the software used for the provision of payment services, including the potential users' payment-related software, is up to date and that critical security patches are deployed.

Payment service providers shall ensure that integrity-checking mechanisms are in place in order to verify the integrity of software, firmware and information on their payment services.

Article 12. *Physical Security*

Payment service providers shall have appropriate physical security measures in place, in particular to protect the sensitive payment data of the users, as well as the ICT systems used to provide payment services.

Article 13. *Access Control*

1. Payment service providers shall ensure that the physical and logical access to ICT systems is permitted only for authorized individuals.

Authorization shall be assigned in accordance with tasks and responsibilities, limited to individuals who are appropriately trained and monitored.

2. Payment service providers shall institute controls that reliably restrict such access to ICT systems to those with a legitimate functional requirement. Electronic access by applications to data and systems should be limited, with respect to the operational staff, to the minimum that is required to provide the relevant service.

3. Payment service providers shall institute strong controls over privileged system access by strictly limiting and closely supervising staff with elevated system access entitlements.

In this respect, controls such as roles-based access, logging and reviewing of the systems activities of privileged users, strong authentication and monitoring for anomalies shall be implemented.

4. Payment service providers shall manage access rights to information assets and their supporting systems on a 'need-to-know' basis. Access rights should be periodically reviewed.

5. Payment service providers shall retain access logs for a period commensurate with the criticality of the identified functions, supporting processes and information assets, in accordance with Article 7, without prejudice to the record-keeping requirements set out in Chapter V of Law No. XVIII of 8 October 2013.

Payment service providers shall use this information to facilitate identification and investigation of anomalous activities that have been detected in the provision of payment services.

6. In order to ensure secure communication and reduce risk, remote administrative access to critical ICT components shall be granted only on a need-to-know basis and when strong authentication solutions are used.

7. Payment service providers shall ensure that the operation of products, tools and procedures related to access control processes shall not be compromised or circumvented. This includes enrolment, delivery, revocation and withdrawal of corresponding products, tools and procedures.

Chapter 4

Detection of Security Breaches

Article 14. *Continuous Monitoring and Detection of Security Breaches*

1. Payment service providers shall adopt and implement processes and capabilities to continuously monitor functions and offices, supporting processes and information assets in order to detect anomalous activities in the provision of payment services.

As part of this continuous monitoring, payment service providers shall have in place appropriate and effective capabilities for detecting physical or logical intrusion, as well as breaches of confidentiality, integrity and availability of the information assets used in the provision of payment services.

2. The continuous monitoring and detection processes shall cover:

a) relevant internal and external factors, including operational and ICT functions;

b) transactions, in order to detect misuse of access by service providers or other entities; and

c) potential internal and external threats.

3. Payment service providers shall adopt and implement detective measures to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities for software and hardware, and check for corresponding new security updates.

Article 15. *Monitoring and Reporting of Operational or Security Incidents*

1. Payment service providers shall determine appropriate criteria and thresholds for classifying an event as an operational or security incident, as well as early warning indicators that should serve as an alert for the payment service provider to enable early detection of operational or security incidents.

2. Payment service providers shall establish appropriate processes and organizational structures to ensure the consistent and integrated monitoring, handling and follow-up of operational or security incidents.

3. Payment service providers shall establish a procedure for reporting such operational or security incidents as well as security-related customer complaints to its management and senior management.

Chapter 5

Operational Continuity

Article 16. *Operational Continuity Management*

1. Payment service providers shall establish sound operational continuity management to maximize their ability to provide payment services on an on-going basis, and to limit losses in the event of severe business disruption.

2. In order to establish sound operational continuity management, payment service providers shall analyse their exposure to severe business disruptions and assess, quantitatively and qualitatively, their potential impact, using internal and/or external data and scenario analysis.

On the basis of the critical functions and offices, processes, systems, transactions and interdependencies identified and classified in accordance with Articles 7 and 8, payment service providers shall prioritise operational continuity actions using a risk-based approach, which can be based on the risk assessments carried out under Chapter 2 of this Title.

Depending on the activity model of the payment service provider, this shall, for example, facilitate the further processing of critical transactions while remediation efforts continue.

3. On the basis of the analysis carried out under paragraph 2, each payment service provider shall put in place:

a) Operational continuity plans to ensure that it can react appropriately to emergencies and is able to maintain its critical activities; and

b) Mitigation measures to be adopted in the event of termination of its payment services and termination of existing contracts, to avoid adverse effects on payment systems and on users, and to ensure execution of pending payment transactions.

4. Operational continuity plans referred to in this Article shall be included in the general operational continuity plan referred to in Article 49 of Regulation No. 1 of 25 September 2014.

5. Payment service providers shall report to the Financial Information Authority the adopted operational continuity plans and mitigation measures, including their updates, within 30 days of the adoption.

Article 17. *Scenario-Based Operational Continuity Planning*

1. Payment service providers shall consider a range of different scenarios, including extreme but plausible ones, to which they might be exposed, and assess the potential impact such scenarios might have.

2. Based on the analysis carried out under Article 16 (2) and plausible scenarios identified under paragraph 1 of this Article, payment service providers shall adopt response and recovery plans, which shall:

a) Focus on the impact on the operation of critical functions and offices, processes, systems, transactions and interdependencies;

b) Be documented and made available to functions and operational offices, and support units and be readily accessible in case of emergency; and

c) Be updated in line with lessons learned from the tests, new risks identified and threats and changed recovery objectives and priorities.

Article 18. *Testing of Operational Continuity Plans*

1. Payment service providers shall test their operational continuity plans, and ensure that the operation of their critical functions and offices, processes, systems, transactions and interdependencies are tested at least annually.

Operational continuity plans shall support objectives to protect and, if necessary, re-establish the integrity and availability of their operations, and the confidentiality of their information assets.

2. Operational continuity plans shall be updated on annual basis, based on testing results, current threat intelligence, information-sharing and lessons learned from previous events, and changing recovery objectives, as well as analysis of operationally and technically plausible scenarios that have not yet occurred, and, if relevant, after changes in systems and processes.

3. In testing their operational continuity plans, payment service providers shall:

a) Include an adequate set of scenarios, as referred to in Article 17 (1);

b) Be designed to challenge the assumptions on which operational continuity plans rest, including governance arrangements and crisis communication plans; and

c) Include procedures to verify the ability of their staff and internal processes to respond adequately to the scenarios above.

4. Payment service providers shall periodically monitor the effectiveness of their operational continuity plans, and document and analyse any challenges or failures resulting from the tests.

Article 19. *Crisis Communication*

In the event of a disruption or emergency, and during the implementation of the operational continuity plans, payment service providers shall ensure that they have effective crisis communication measures in place so that all relevant internal and external stakeholders are informed in a timely and appropriate manner.

Chapter 6

Testing of Security Measures

Article 20. *Reference Framework for the Testing of Security Measures*

1. Payment service providers shall adopt and implement a testing framework that validates the robustness and effectiveness of the security measures, and ensure that the testing framework is adapted to consider new threats and vulnerabilities, identified through risk-monitoring activities.

2. The testing framework should also encompass the security measures relevant to:

a) Payment terminals and devices used for the provision of payment services;

b) Payment terminals and devices used for authenticating the users; and

c) Devices and software provided by the payment service provider to the user to generate/receive an authentication code.

3. The testing framework shall ensure that tests:

a) Are performed as part of the payment service provider's formal change management process to ensure their robustness and effectiveness;

b) Are carried out by independent testers who have sufficient expertise in testing security measures of payment services and are not involved in the development of the security measures for the corresponding payment services or systems that are to be tested, at least for final tests before putting security measures into operation; and

c) Include vulnerability scans and penetration tests adequate to the level of risk identified with the payment services.

Article 21. *Testing of the Security Measures*

1. Payment service providers shall carry out on-going and repeated tests of the security measures for their payment services.

For systems that are critical for the provision of their payment services, as identified consistently with the provisions of Article 7 (2), these tests shall be performed at least on an annual basis. Non-critical systems shall be tested regularly on a risk-based approach, but at least every three years.

2. Payment service providers shall ensure that tests are carried out in the event of changes of infrastructure, processes or procedures, and if changes are made as a consequence of major operational or security incidents.

3. Payment service providers shall monitor and evaluate the results of the tests carried out, and update their security measures accordingly and without delay.

4. Payment service providers shall report to the Financial Information Authority the results of the tests carried out, within 30 days of the results, and the possible corrective measures adopted.

Chapter 7

Situational Awareness and Continuous Learning

Article 22. *Threat Landscape and Situational Awareness*

1. Payment service providers shall adopt and implement processes and organizational structures to identify and constantly monitor security and operational threats that could materially affect their ability to provide payment services.

2. Payment service providers shall analyse operational or security incidents that have been identified or have occurred within and/or without the entity.

Payment service providers shall consider key lessons learned from these analyses and update the security measures accordingly.

3. Payment service providers shall actively monitor technological developments to ensure that they are aware of security risks.

Article 23. *Training and Security Awareness Programmes*

1. Payment service providers shall adopt and implement a training programme for all staff to ensure that they are trained to perform their duties and responsibilities consistent with the relevant security policies and procedures in order to reduce human error, theft, fraud, misuse or loss.

Payment service providers shall ensure that the training programme provides for training staff members at least annually, and more frequently if required.

2. Payment service providers shall ensure that staff members occupying key roles identified under Article 7 (1) receive targeted information security training on an annual basis, or more frequently if required.

3. Payment service providers shall adopt and implement periodic security awareness programmes in order to educate their personnel and to address information security related risks. These programmes should require payment service providers' personnel to report any unusual activity and incidents.

Chapter 8

Payment service User Relationship Management

Article 24. *Payment Service User Awareness on Security Risks and Risk-Mitigating Actions*

1. Payment service providers shall adopt and implement processes to enhance users' awareness of security risks linked to the payment services, by providing users with assistance and guidance.

2. The assistance and guidance offered to users shall be updated in the light of new threats and vulnerabilities, and changes shall be communicated to the users.

3. Payment service providers shall provide users with the option to receive alerts on initiated and/or failed attempts to initiate payment transactions, enabling them to detect fraudulent or malicious use of their account.

4. Payment service providers shall keep users informed about updates in security procedures, which affect users regarding the provision of payment services.

5. Payment service providers shall provide users with assistance on all questions, requests for support and notifications of anomalies or issues regarding security matters related to payment services. Users shall be appropriately informed about how such assistance can be obtained.

Title III

Classification and Notification of Major Operational or Security Incidents

Chapter 1

Incident Classification Criteria

Article 25. *General Principles*

1. Payment service providers shall assess an operational or security incident against the criteria referred to in Article 26.

2. The assessment referred to in paragraph 1 is aimed at determining the impact level – "negligible", "lower" or "higher" – for each individual criterion, consistently with the provisions of Article 28.

3. An operational or security incident is classified as major if, on the basis of the determination of the impact levels referred to in paragraph 2, it is observed that:

a) One or more criteria have an "higher" impact level, or

b) Three or more criteria have a "lower" impact level'.

Article 26. *Reference Criteria and Indicators*

1. Payment service providers shall assess an operational or security incident against the following criteria and their underlying indicators.

a) *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.

b) *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.

c) *Service Downtime*

Payment service providers shall determine the period of time when the service will probably be unavailable for the payment service user or when the payment order cannot be fulfilled by the payment service provider.

d) *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 capital).

e) *High Level of Internal Escalation*

Payment service providers shall determine whether or not this incident has been or will probably be reported to their management or senior management.

f) *Other Payment Service Providers or Relevant Infrastructures Potentially Affected*

Payment service providers shall determine the potential spillover of the incident beyond the initially affected payment service provider to other payment service providers, financial market infrastructures, and/or card payment schemes.

g) *Reputational Impact*

Payment service providers shall determine how the incident can undermine users' trust in the payment service provider itself.

Article 27. *Calculation Methodology for the Underlying Indicators of the Reference Criteria*

1. Payment service providers shall calculate the value of the indicators according to the following methodology.

a) *Transactions affected*

As a general rule, payment service providers shall consider all domestic and cross-border transactions that have been or will probably be directly or indirectly affected 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 (whether the funds have been recovered or not).

Furthermore, payment service providers shall understand the regular level of payment transactions to be 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 payment service providers do not consider this figure to be representative (for instance because of seasonality), they can use another, more representative, metric instead, and convey to the Financial Information Authority the underlying rationale for this approach in the corresponding field of the reporting template (Annex 1).

b) *Payment Service Users Affected*

Payment service providers shall consider all users that have a contract that grants them access to the affected payment service, and that have suffered or will probably suffer the consequences of the incident.

Payment service providers shall resort to estimations based on past activity to determine the number of payment service users that may have been using the payment service during the lifetime of the incident.

Furthermore, payment service providers shall take as the total number of payment service users the aggregated figure of payment service users contractually bound to 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.

c) *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 probably be down and, thus, prevents:

i) The initiation and/or execution of a payment service; and/or

ii) Access to a payment account.

Payment service providers shall count the service downtime from the moment the downtime starts, and they shall consider both the time of 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.

d) *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. Among other things, payment service providers shall 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. As regards the indirect costs, payment service providers shall consider only those that are already known or very likely to materialize.

e) *High Level of Internal Escalation*

Payment service providers shall consider whether or not, as a result of its impact on payment-related services, the management or the senior management have been or will probably be informed about the incident outside any periodical notification procedure, and on a continuous basis throughout the lifetime of the incident.

Furthermore, payment service providers shall consider whether or not, as a result of the impact of the incident on payment-related services, a crisis mode has been or is likely to be triggered.

f) *Other Payment Service Providers or Relevant Infrastructures Potentially Affected*

Payment service providers shall assess the impact of the incident on the financial market infrastructures and/or card payment schemes that support them and other payment service providers.

In particular, payment service providers shall assess whether or not the incident has been or will probably be replicated at other payment service providers, whether or not it has affected or will probably affect the smooth functioning of financial market infrastructures and whether or not it has compromised or will probably compromise the sound operation of the financial system as a whole.

Payment service providers shall 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, and whether or not the payment service provider has stopped or will probably stop fulfilling its obligations in the financial market infrastructures of which it is a member.

g) *Reputational Impact*

Payment service providers shall consider the level of visibility that, to the best of their knowledge, the incident has gained or will probably gain.

In particular, payment service providers shall consider the likelihood that the incident will cause harm to the entity as a good indicator of its potential to affect their reputation. Payment service providers shall take into account whether or not (i) the incident has affected a visible 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.), (ii) regulatory obligations have been or will probably be missed, (iii) sanctions have been or will probably be breached or (iv) the same type of incident has occurred before.

Article 28. *Determination of the Impact Level*

1. Payment service providers shall assess an incident by determining, for each individual criterion, if the relevant thresholds in Table 1 are or will probably be reached before the incident is resolved.

2. Payment service providers can resort to estimations if they do not have actual data to support their judgments of whether or not a given threshold is or will probably be reached before the incident is resolved (for instance, this could happen during the initial investigation phase).

3. Payment service providers shall carry out this assessment on a continuous basis during the lifetime of the incident, to identify any possible status change, either upwards (from non-major to major) or downwards (from major to non-major).

Table 1 – *Thresholds*

Criteria	Lower impact level	Higher impact level
Transactions affected	> 10% of the payment service provider's regular level of transactions (in terms of number of transactions) or > 100,000 euros	> 25% of the payment service provider's regular level of transactions (in terms of number of transactions) or > 5 million euros
Payment service users affected	> 500 or > 10 % of the payment service provider's payment service users	> 5,000 or > 25 % of the payment service provider's payment service users
Service downtime	> 2 hours	> 1 day
Economic impact	Not applicable	> Max (0.1 % capital, 200,000 euros) or > 5 million euros
High level of internal escalation	Yes	Yes, and a crisis mode is likely to be activated
Other payment service providers or related infrastructures potentially involved	Yes	Not applicable
Reputational impact	Yes	Not applicable

Chapter 2

Notification Process

Article 29. *General Principles*

1. Payment service providers shall collect all relevant information, produce an incident report using the template provided in Annex 1, and submit it to the Financial Information Authority.

Payment service providers shall fill out the template following the instructions provided in Annex 2.

2. Payment service providers shall use the same template referred to in paragraph 1 to inform the Financial Information Authority throughout the lifetime of the incident (i.e. for initial, intermediate and final reports).

Payment service providers shall complete the template in an incremental manner, on a best effort basis, as more information becomes readily available in the course of their internal investigations.

3. Payment service providers shall present to the Financial Information Authority a copy of the information provided (or that will be provided) to their users, as soon as it is available.

4. Payment service providers shall provide to the Financial Information Authority, if available and deemed relevant, with any additional information by appending supplementary documentation to the template provided in Annex 1 as one or various annexes.

5. Payment service providers shall follow up on any requests from the Financial Information Authority to provide additional information or clarifications regarding already submitted documentation.

6. Payment service providers shall at all times preserve the confidentiality and integrity of the information exchanged with the Financial Information Authority.

Article 30. *Initial Report*

1. Payment service providers shall submit an initial report to the Financial Information Authority when a potential major operational or security incident is first detected.

2. Payment service providers shall send the initial report referred to in paragraph 1 within 4 hours of the moment the potential major operational or security incident was first detected, or, if the reporting channels are known not to be available or operational at that time, as soon as they become available/operational again.

3. Payment service providers shall submit an initial report referred to in paragraph 1 when a previously non-major incident becomes a major incident. In this particular case, payment service providers shall send the initial report immediately after the change of status is identified, or, if the reporting channels are known not to be available or operational at that time, as soon as they become available/operational again.

4. Payment service providers shall include headline-level information (i.e. section A of the template provided in Annex 1) in their initial reports, thus featuring some basic characteristics of the incident and its expected consequences based on the information available immediately after it was detected or reclassified.

Payment service providers can resort to estimations when actual data is not available.

Payment service providers shall also include in their initial report the date for the next update, which should be as soon as possible, and under no circumstances go beyond 3 business days.

Article 31. *Intermediate Report*

1. Payment service providers shall submit intermediate reports every time they consider that there is a relevant status update and, as a minimum, by the date for the next update indicated in the previous report (either the initial report or the previous intermediate report).

2. Payment service providers shall submit to the Financial Information Authority a first intermediate report with a more detailed description of the incident and its consequences (section B of the template provided in Annex 1).

Moreover, payment service providers shall produce additional intermediate reports by updating the information already provided in sections A and B of the template provided in Annex 1 at least, when they become aware of new relevant information or significant changes since the previous notification (e.g. whether the incident has escalated or decreased, new causes identified or actions taken to fix the problem).

In any case, payment service providers shall produce an intermediate report every time at the request of the Financial Information Authority.

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

4. Payment service providers shall indicate in each intermediate report the date for the next update, which should be as soon as possible, and under no circumstances go beyond 3 business days.

If the payment service provider is not be able to comply with the estimated date for the next update, it should send a formal communication to the Financial Information Authority in order to explain the reasons behind the delay, propose a new plausible submission deadline (no longer than 3 business days) and send a new intermediate report updating exclusively the information regarding the estimated date for the next update.

5. Payment service providers shall send the last interim communication when normal operations have been restored and the activity has returned to normal, informing the Financial Information Authority of the circumstance.
Payment service providers shall consider that activity is back to normal when activity/operations are restored to the same level of service/conditions prior to the incident in terms of processing times, capacity, security requirements, etc., and contingency measures are no longer in place.

6. If activity is back to normal before 4 hours have passed since the incident was detected, payment service providers shall aim to submit both the initial and the last intermediate report simultaneously (i.e. filling out sections A and B of the template provided in Annex 1) by the 4-hour deadline.

Article 32. *Final Report*

1. Payment service providers shall send to a final report when the root cause analysis has taken place (regardless of whether or not mitigation measures have already been implemented or the final root cause has been identified) and there are actual figures available to replace any estimates.

2. Payment service providers shall deliver the final report to the Financial Information Authority within a maximum of 2 weeks after the activity is deemed back to normal.

Payment service providers needing an extension of this deadline (e.g. if there are no actual figures on the impact available yet) shall send a formal request to the Financial Information Authority before it has lapsed, providing an adequate justification for the delay, as well as a new estimated date for the final report.

3. If payment service providers are be able to provide all the information required in the final report (i.e. section C of the template provided in Annex 1) within the 4-hour window since the incident was detected, they shall aim to submit in their initial report the information related to initial, last intermediate and final reports.

4. Payment service providers shall include in their final reports full information, i.e.:

a) Actual figures on the impact instead of estimations (as well as any other update needed in sections A and B of the template provided in Annex 1); and

b) Section C of the template provided in Annex 1, which includes the root cause, if already known, and a summary of measures adopted or planned to be adopted to remove the problem and prevent its recurrence in the future.

5. Payment service providers shall send a final report to the Financial Information Authority 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 major and is not expected to fulfil them before the incident is resolved.

In this case, payment service providers shall send the final report as soon as this circumstance is detected and, in any case, by the estimated date for the next report. In this particular situation, instead of filling out section C of the template provided in Annex 1, payment service providers shall tick the box 'incident reclassified as non-major' and explain the reasons justifying this downgrading.

Article 33. *Reporting Methods*

The reports referred to in this Chapter shall be send to the institutional e-mail address of the Office for Supervision and Regulation of the Financial Information Authority: uvr@aif.va.

Title IV

Final provisions

Article 34. *Final Provisions*

1. In case of violation or non-compliance with the provisions established by this Instruction, the Financial Information Authority may apply the administrative sanctions established by Article 69 of Regulation No. 3 of 23 May 2018.

2. The Financial Information Authority updates this Instruction consistently with the development of the institutional, legal, economic, commercial and professional framework of the State, also taking into account what established by the relevant international and European bodies.

This Instruction, including Annexes, will enter into force on the day of its publication in the official website of the Financial Information Authority.

Vatican, 29 May 2019

RENÉ BRÜLHART
President

Visto

TOMMASO DI RUZZA
Director