LATVIJAS BANKA
EIROSISTĒMA

Guidelines for monitoring, managing and mitigating the risk of financial fraud

Contents

1. General Provisions

1.1. Latvijas Banka has developed guidelines for credit institutions, payment institutions, electronic money institutions, and all branches of such Member State entities in the Republic of Latvia (hereinafter referred to as the "Institution") to monitor, manage and mitigate the risk of financial fraud (hereinafter referred to as the "fraud risk"). Each Institution applies the explanations provided in the guidelines to the extent that they align with its operational specifics, the services it provides, and the products it offers, while also considering the risks inherent in its operations.

1.2. These guidelines have been issued pursuant to Section 48, Paragraph three of the Law on Payment Services and Electronic Money, Section 50, Paragraph two of the Credit Institution Law, and Section 46, Paragraph one, Clause 2 of the Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing.

1.3. The guidelines have been developed in accordance with the applicable laws and regulations, as well as best practices in effect at the time of their drafting and updates.

1.4. The guidelines have been issued to provide explanations regarding the organisational requirements for the internal management of fraud risk, the conditions of its management, the efficiency of the complaint review process, and the procedure for rejecting payment orders, including the suspension of payments, as well as recommendations concerning the requirements for information availability and exchange between the Institutions involved in combating financial fraud. The guidelines include the "comply or explain" principle, considering the different operating models of Institutions and their affiliation with various groups of financial institutions, including cross-border financial groups.

1.5. The content of the guidelines has been developed in accordance with the basic principles of fraud risk management and mitigation. The guidelines include explanations about the scope and scale of the measures to be taken depending on the risk, as well as explanations about specific fraud risk management and mitigation measures, for which a unified understanding of the basic principles is required in their application.

1.6. The purpose of the guidelines is to strengthen the principles of fraud risk mitigation, as well as to develop a unified approach to fraud risk management using a risk-based approach. A risk-based approach means that the Institution

identifies, assesses, and understands the fraud risk and applies management measures to the fraud risk according to the risk it is exposed to, with the aim of effectively managing this risk.

1.7. The guidelines may not be used as a basis for claims for compensation of losses in disputes between the Institution and its customer. Compensation of losses is governed by external regulatory acts.

1.8. Fraud risk management measures are established based on the risk assessment, i.e. assessment of the risk inherent in the Institution's operations and of that inherent in fraud. This principle is explained with examples in the respective sections of the guidelines. Considering that each Institution offers different products and services, the risk inherent in its operations and that inherent in fraud cases vary. As a result, the measures implemented by one Institution may differ from those of another.

1.9. The content of the guidelines will be refined and supplemented in accordance with the issues and examples of best practice identified. Examples serve as explanatory information and cannot be uniformly applied to all cases without evaluation, as each situation may differ. While the actual conditions may initially seem similar to those mentioned in the examples, they can differ when evaluating the details of the actual conditions. As a result, the Institution may need to implement measures that differ from those mentioned in the examples or introduce additional ones.

2. Organisational Requirements for Internal Management of Fraud Risk

2.1. Strong internal governance and effective internal processes are essential to protect the Institution and its customers from external financial fraud. The Institution can minimise fraud risk and safeguard its assets and reputation more effectively by adopting a systemic approach and a unified framework for monitoring, managing, and mitigating fraud risk, by clearly defining roles and responsibilities of the relevant persons, functions, bodies within the internal governance and establishing management accountability, and by implementing effective oversight mechanisms, fostering an inclusive culture, and leveraging technological capabilities and data analysis.

2.2. When determining external and internal factors critical to the Institution's objectives and its ability to successfully monitor, manage, and mitigate fraud risk, the Institution identifies the relevant stakeholders and their requirements for the expected developments and outcomes in mitigating and preventing financial

fraud. The responsibility and role of the Institution's management, along with the expected risk culture it upholds through a tone-from-the-top approach, are crucial for ensuring appropriate internal control mechanisms and effective processes for identifying, managing, monitoring, and reporting fraud risk.

2.3. To establish and maintain effective processes and controls for fraud risk prevention, the Institution defines and documents a clear allocation of roles and responsibilities:

2.3.1. the management of the Institution is fully responsible for assessing the fraud risk, implementing prevention measures, which are an essential part of the overall risk management system, as well as for determining reasonable risk appetite and assuming residual risk. Similarly, the Institution's management is responsible for promoting awareness and ensuring that all involved employees clearly understand the Institution's overall framework for fraud risk prevention and the related processes, as well as their role and obligations in these processes;

2.3.2. the Institution's management appoints the structural unit or employees directly responsible for ensuring the fraud risk prevention processes.

2.4. The Institution develops and implements a fraud risk management framework that outlines processes requiring close collaboration and regular information exchange between the structural units involved in financial fraud prevention and the internal control functions (the second and third lines of defence), as well as, when necessary, with external auditors. The Institution's fraud risk management framework, which includes policies, procedures, and risk mitigation and control measures, is clearly defined, documented, and is regularly (preferably every year) reviewed and updated.

2.5. To effectively manage fraud risk, the Institution identifies the categories (groups) of its employees who must receive regular training in fraud risk and its prevention (management). Taking into account the knowledge and qualifications required for the employees' job duties, responsibilities, and level of authorisation, the Institution ensures that these employees:

2.5.1. are informed about the types and prevention methods of fraud risk;

2.5.2. understand the regulatory requirements for fraud risk management, including industry-specific rules and standards;

2.5.3. regularly acquire specific knowledge on identifying, assessing, and mitigating fraud risk;

2.5.4. gain the necessary hands-on experience with fraud risk management systems and procedures;

2.5.5. regularly enhance their competencies to stay informed about the latest trends and best practices in fraud risk management;

2.5.6. participate in training that helps improve knowledge and skills related to fraud risk management.

2.6. Institutions agree on and maintain a secure, reliable information exchange system that facilitates mutual exchange of financial fraud information to enhance transaction monitoring capabilities. The exchange of current information is ensured immediately (in real-time). When exchanging financial fraud data, Institutions go beyond just the payment recipient's unique identifiers or the International Bank Account Number (IBAN), incorporating additional data whenever possible. While Information exchange should primarily focus on the national (domestic) level, Institutions may voluntarily exchange data between countries in a cross-border context, if this is necessary and compliance with regulatory requirements is ensured.

2.7. The Institution establishes the procedure and designates the responsible persons for immediately reporting fraud incidents in the digital environment to the Cyber Incident Response Institution CERT.LV, including providing information available to the Institution about the domain name or the website involved in the specific fraud case. Based on the relevance of the information, the Institution assesses whether immediate reporting is necessary.

2.8. To ensure effective fraud risk management, the Institution defines, documents, and regularly (at least once a year) reviews the fraud risk management strategy, the risk tolerance level, and the quantitative or qualitative indicators of the risk level. To identify potential risk or changes in the risk level, the Institution establishes and regularly reviews the key risk indicators (KRIs). To evaluate the effectiveness of the fraud risk management process, the Institution establishes and regularly reviews the key performance indicators ("KPIs"). All indicators are reviewed regularly (at least once a year). By calibrating indicators and setting their materiality thresholds, the Institution ensures its ability to identify when additional measures are needed to implement changes or improvements in its operational process. The Institution establishes a process for effective oversight, monitoring, communication, and evaluation of the indicators at the highest management level.

2.9. Based on the risk management performance indicators for financial fraud detection and prevention, the Institution's management regularly (at least once a year) reviews and assesses the adequacy of the personnel and technical resources required to prevent financial fraud. Additionally, the management plans and allocates the necessary funding, taking into account the risk management performance indicators.

2.10. The Institution regularly (at least once a year) conducts a self-assessment of the effectiveness of the financial fraud detection and prevention process, taking into account the internal and external factors that may influence fraud case statistics, including financial fraud statistics compiled in accordance with the requirements of Latvijas Banka's Regulation No 208 "Regulation on Compiling and Submitting the Statistical Data on Customer Payments" of 13 June 2022. The assessment also evaluates the adequacy of personnel and information technology resources, as well as the effectiveness of fraud risk management in meeting organisational requirements, following risk management procedures, and achieving fraud prevention objectives. The Institution's risk management or compliance function and the management bodies (senior management) are informed about the self-assessment results and the measures taken to address any identified deficiencies.

2.11. The Institution's senior management periodically reviews its chosen approach to monitoring, managing, and mitigating fraud risk, along with the associated framework, to ensure continued suitability, effectiveness, and alignment with the Institution's strategic objectives. The Institution's management takes into account at least the following:

2.11.1. changes in external and internal factors that impact the Institution's ability to achieve its intended outcomes in fraud risk monitoring, management, and mitigation;

2.11.2. information on the effectiveness of fraud risk monitoring, management, and mitigation processes;

2.11.3. report results of previous management reviews on fraud risk;

2.11.4. results of internal and external audits, as well as compliance inspections, including those related to information technology management and security;

2.11.5. trends emerging from the results of financial fraud mitigation and prevention efforts, resource adequacy, monitoring and measurement outcomes, controls implemented to address operational efficiency risks, and emerging methods and schemes used by fraudsters, etc.

2.12. The results indicated in the management reports include the decisions and actions that determine:

2.12.1. the instructions on any necessary changes to the chosen approach for monitoring, managing, and mitigating fraud risk, as well as its framework;

2.12.2. the opportunities to improve and enhance processes and technological solutions;

2.12.3. resource requirements.

2.13. Considering that the existing fraud threats are increasing and new ones are emerging, fuelled by the misuse of artificial intelligence and the development of new fraud schemes by financial fraudsters, the Institution implements appropriate technological and organisational measures to enhance the efficiency of the payment transaction monitoring process and reduce the number of financial fraud cases. This includes enhancing the timely detection of potential fraud, for instance, in cases where customers have not yet realised that their authentication data have been compromised or that identity data or payment instrument theft has occurred. Therefore, in the context of payment transaction monitoring, the Institution establishes appropriate risk estimates for payment transactions or employs equivalent alternative solutions for grouping payment transactions into specific risk levels, selecting appropriate control procedures and risk mitigation measures for each level, ranging from implementing strong customer authentication (SCA) for payment transaction approval or executing payments only after the customer's confirmation, to suspending or refusing the transaction.

2.14. The Institution leverages technological solutions within its capabilities to mitigate and prevent financial fraud, ensuring that the invested funds and resources are justified. These solutions also ensure that the stakeholders' requirements regarding the expected outcomes are met, including fostering customer trust in the Institution and meeting Latvijas Banka's expectations for financial market security. For this purpose, the Institution identifies potential actions whose effectiveness could be measured and monitored in the context of the technological solution's operation. These measurements should be repeatable, allowing for comparison and verification of results.

2.15. The Institution's risk control function regularly conducts in-depth, independent, and comprehensive fraud risk measurement, assessment, and monitoring, as well as an analysis of the effectiveness of fraud risk prevention processes or measures. The findings are then reported to the Institution's management.

2.16. The Institution sets requirements for the systematic and regular risk-based (justified) involvement of internal audit in the oversight of the financial fraud detection and prevention process:

2.16.1. the Institution mandates the inclusion of financial fraud matters in the internal audit work plans, taking into account the results of fraud risk monitoring and review, reported performance outcomes of fraud risk monitoring, management and mitigation processes, planned regulatory and the Institution's procedural changes, as well as results of previous audits;

2.16.2. the Institution establishes the criteria and scope for each audit to be conducted and engages auditors with appropriate competences to conduct the planned audits;

2.16.3. the Institution ensures that audit results are submitted to its management and that corrective measures for fraud risk are determined in a timely manner, and their implementation is monitored.

3. Fraud Risk Management

3.1. To ensure that the objectives and expected results are achieved and the undesirable impact of the identified risks is prevented or mitigated, the Institution takes into account the requirements set out in Chapter 2 of these guidelines and carries out an assessment of current fraud risk at least once a year, using its chosen methodology for conducting a fraud risk assessment. This methodology must include requirements for conducting a documented fraud risk assessment and preparing a risk assessment (explanation of the assessment's objective, scope, and procedure). It must also establish a procedure for submitting fraud risk assessment results for senior management review.

3.2. The Institution systematically and iteratively conducts fraud risk assessments in collaboration with field experts, leveraging their knowledge and insights, using the most relevant available information, and ensuring that:

3.2.1. the conducted fraud risk assessment is documented and the obtained results are reliable and comparable;

3.2.2. all current risks are identified and described, based on reliable information and reasoning that the aforementioned risks could limit the Institution's capabilities or prevent it from achieving the specified objectives for monitoring, management, and mitigation of fraud risk. It should be noted that the sources of the identified risks may not fall within the Institution's scope of oversight;

3.2.3. the analysis of the identified fraud risk is carried out using qualitative or quantitative methods or a combination thereof to ensure that the obtained results provide an understanding of decisions that justify the choices made based on the respective risk levels. The fraud risk assessment includes information about the overall level of fraud risk, its changes, and the main factors affecting it, including information about newly identified fraud typologies, as well as the Institution's ability to effectively manage the newly identified risk types and risk level changes. The Institution regularly monitors statistical data available in accordance with the Guidelines on fraud reporting under PSD2 (Directive (EU) 2015/2366) of the European Banking Authority, assessing its overall fraud risk

level for key payment instruments against the maximum permissible threshold set by the European Union;

3.2.4. the prepared fraud risk assessment must include a comparison of the results of the risk analysis with the established risk acceptance criteria, to identify situations where further actions are necessary concerning the residual risk, taking into account the broader context and actual consequences for the stakeholders interested in the Institution's fraud risk management;

3.2.5. the results of the fraud risk assessment are recorded and communicated to the Institution's management.

3.3. Based on the results of the fraud risk assessment and the efficiency assessment of financial fraud detection and prevention processes (self-assessment), the Institution establishes or updates fraud mitigation objectives and the planned activities to achieve them. It also defines the frequency of monitoring the implementation progress and designates the persons responsible for executing these activities:

3.3.1. the Institution develops fraud risk management plan to ensure that the chosen risk management options will be implemented in order for the parties involved in fraud risk management to understand the specified measures and be able to track the implementation of this plan;

3.3.2. the fraud risk management plan clearly sets out the procedure for implementing risk management and integrating it into the Institution's management plans and processes, in agreement with the relevant stakeholders.

3.4. In accordance with best practices in fraud risk management, it is advisable for the Institution to implement the most appropriate options when planning to balance potential benefits with the achievement of fraud mitigation objectives and implementation costs, including efforts invested in addressing deficiencies that cannot be completely eliminated. These options are not always mutually exclusive or suitable in all circumstances. Therefore, the Institution's management and other stakeholders must be aware of the type and extent of the residual risk after risk assessment, and the residual risk must be documented and subjected to monitoring, review, and, if necessary, further assessment. However, if risk management options are unavailable or do not adequately change the risk level, the respective risk must be documented, and its magnitude must be continuously reviewed.

3.5. The Institution takes into account that even carefully designed and implemented risk management may not yield the expected results and may have unforeseen consequences. Therefore, continuous monitoring and review of the registered risks are essential to promptly detect when existing risk management

measures become ineffective. Moreover, these planned risk management measures may create new risks, which must also be managed accordingly. Therefore, the ongoing monitoring and periodic review of the risk management process and its outcomes must be an integral part of the risk management process, with clearly defined responsibilities at all stages of the process, including planning, information gathering and analysis, recording outcomes, and providing feedback.

3.6. The Institution ensures that the effectiveness of processes and controls implemented to prevent financial fraud is systematically evaluated and that the obtained evaluation results are documented and retained. The Institution analyses and assesses the relevant data and information derived from monitoring and measurement results. For this purpose, the Institution establishes:

3.6.1 measurable parameters to be periodically monitored and measured, and the methods of fraud monitoring, measurement, analysis, and assessment that ensure the acquisition of valid results;

3.6.2. the periods for conducting fraud monitoring and measurement and for analysing and assessing the fraud monitoring and measurement results;

3.6.3. the persons responsible for conducting fraud monitoring assessments and maintaining documentation.

3.7. The Institution uses the results of fraud monitoring analysis to assess:

3.7.1. the effectiveness of planning the chosen approach and framework for monitoring, managing, and mitigating fraud risk, including the adequacy of human and technical resources;

3.7.2. the operational effectiveness of financial fraud prevention processes and controls;

3.7.3. the effectiveness of actions taken to prevent fraud risk;

3.7.4. the need for improvements in the monitoring, management, and mitigation of fraud risk.

3.8. The Institution employs the most suitable and advanced technological solutions available in the prevention of financial fraud, ensuring:

3.8.1. alongside the already known fraud prevention scenarios, the capacity to quickly incorporate newly identified fraud prevention scenarios and to integrate payment transaction indicators into additional monitoring scenarios;

3.8.2. the use of historical usage data to identify unusual customer behaviour when performing activities through internet banking or the mobile application;

3.8.3. interaction between different levels of fraud risk and risk-based factors (e.g., installation of a mobile application on another device, digitisation of a payment card, etc.) and the possibilities of grouping transactions according to the respective risk level, implementing fraud risk monitoring, management, and mitigation.

3.9. The Institution ensures that in the payment transaction monitoring process, upon detecting the registration of new payment instruments, such as the addition of a payment card to a smart device's digital wallet, and their use, as well as in cases of high and increased risk, the interaction between different risk levels and risk-based factors is taken into account, considering the available data. If applicable and technically feasible, these principles also apply to e-commerce transactions, including with merchants outside the European Union. In the process of monitoring payment transactions in general and in the aforementioned cases in particular, based on the specifics of the payment execution, strong customer authentication should be the default requirement and the following should be considered:

3.9.1. when performing online banking authentication, a device is used for which the Institution has no information regarding its technological parameters or previous usage. Considering other risk-enhancing factors in such cases, it is advisable that the Institution assigns an elevated risk level to ongoing transactions, including e-commerce purchases and payments between customer accounts – particularly when funds are transferred to an account linked to a debit or credit card and subsequently used for e-commerce transactions;

3.9.2. it has been detected that a new payment instrument, such as a mobile application, has been installed, or a customer's payment card has been added to a digital wallet on a device not previously recognised by the Institution. In such cases, it is advisable that the Institution foresees and implements a procedure for registering a new device of a customer. For instance, a notification could be sent to the customer's previously registered device requiring additional approval before the new device can be used with the application or before authorising the digitalisation of the customer's card. Alternatively, the Institution may employ other equivalent solutions that clearly inform the customer about the registration of a new device;

3.9.3. it has been detected that payment transactions have been executed evoking suspicion of potential fraud. For example, an unusually large number of payment orders involving credit or debit funds within the respective payment account, particularly in cases where the total value of the submitted payment orders is equivalent to the account balance. Other suspicious indications include payment orders initiated at atypical times or involving unusually large amounts for the

customer, rapid fund withdrawals, including withdrawals in foreign currency or purchases of crypto assets, as well as payment order details and payment execution features such as uncharacteristic language use, and disproportionately fast text input speed, indicative of order generation using automated, technological tools, etc.;

3.9.4. payment orders have been submitted from a location uncharacteristic for the customer, including when payment orders have been received by the Institution from geographically distant locations within a short period of time;

3.9.5. it has been detected that information technology tools, IP addresses, and other technological means previously associated with violations have been used. This includes cases where the Institution itself or other reliable information sources already have such information;

3.9.6. the Institution itself or other reliable information sources have detailed information on previously detected fraud cases, such as the payment accounts used in fraud and their parameters or the parties involved in the fraud cases and schemes;

3.9.7. it has been detected that anomalies exist in the network parameters of the devices used for access, payment instruments have been used simultaneously from different IP addresses, there has been rapid switching between IP addresses from different subnets, and there are signs of virtual private network (VPN) and proxy server use, etc.;

3.9.8. signs of malware presence have been identified at any stage of the customer authentication process;

3.9.9. transactions have been conducted between the payer and a payee that may be considered trusted; however, the payee was not listed in the Institution's register of trusted transaction partners at the time of the transaction;

3.9.10. cases when fraud suspicions have been reported, etc.

3.10. As part of transaction monitoring, the Institution monitors incoming payments to the extent possible, considering its technological capabilities, for non-standard transactions such as the use of quick loans, payments with incorrect credentials, and attempts to transfer funds further.

4. Efficiency of the Complaint Review Process

4.1. The Institution establishes the procedure for reviewing financial fraud complaints and organises the review of complaints in accordance with Latvijas Banka's Regulation No 358 "Procedure for Managing Complaints Received by Financial Market Participants" of 2 December 2024.

4.2. Upon receiving information about a financial fraud case in which the customer disputes a transaction (including cases reported via the call centre), the Institution conducts a situation analysis:

4.2.1. the Institution strictly monitors and analyses all complaints it receives regarding possible financial fraud, including cases where fraud is suspected;

4.2.2. the Institution conducts an analysis of the received complaints, which can help it develop profiles of potential fraudsters, the typologies characteristic of their activities, and the criteria for identifying such actions, which will enhance the monitoring process;

4.2.3. to improve the effectiveness of the implemented fraud prevention measures, the Institution continuously monitors the statistics of the received complaints, comparing them with the overall available customer base, as well as the available information on the number of complaints submitted regarding cross-border payments, and keeps track of changes in the risk level based on the key risk indicators determined for each item.

4.3. Upon reviewing information regarding financial fraud in which a customer disputes a transaction, the Institution:

4.3.1. carefully evaluates the information available to fully assess the circumstances of the fraud and, if necessary, requests additional information from the customer;

4.3.2. identifies the circumstances of the committed fraud and the actions of the customer.

4.4. When responding to complaints about financial fraud, the Institution adheres to the following principles, in addition to the general procedure for preparing responses to complaints:

4.4.1. the response is provided in detail regarding the specific customer's case;

4.4.2. the response is delivered with accurate spelling, ensuring no errors in the description of the sequence of events;

4.4.3. a general response with standard phrases is not permissible, including merely citing contract clauses without explanation; instead, it should be detailed how exactly the fraud occurred and where the customer exhibited gross negligence, which could have been avoided;

4.4.4. in the event of a refusal of compensation (loss coverage), a justification for the refusal is provided. If the reason for refusal is the customer's gross negligence, the Institution provides a detailed assessment of the circumstances of gross negligence;

4.4.5. the answer is provided in clear and understandable language (with the shortest, most specific sentences possible).

4.5. Upon request from the supervisory authority, when providing an explanation regarding a financial fraud complaint, the Institution includes:

4.5.1. an explanation of the actions the Institution has taken in relation to the complaint, including the recovery of funds;

4.5.2. detailed technical information about the fraud case;

4.5.3. evidence and conclusions regarding the customer payment authorisation;

4.5.4. if applicable to the actual circumstances of the specific complaint – an assessment of whether the payment was made by the customer acting unlawfully with malicious intent or due to gross negligence;

4.5.5. if applicable to the actual circumstances of the specific complaint – in a situation where the customer is involved as a money mule in the particular case, the customer research file, which includes information and supporting documentation on customer identification, initial customer research, risk level (its changes), regular customer research, and transaction monitoring.

5. Rejection of Payment Orders (Suspension and Cancellation of Payments)

5.1. In addition to the general transaction monitoring procedure, the Institution adheres to the following conditions for monitoring and rejecting transactions:

5.1.1. if the Institution detects before executing a transaction that a payment or instant payment carries a high risk, it refuses to accept such a payment for execution and notifies the customer thereof, including providing a general reason for the refusal;

5.1.2. taking into account the habits and risk profile of the customer group, including the risk factors referred to in Paragraph 3.9 of these guidelines, the Institution sets various initial limits when starting to provide payment services to a customer. Furthermore, it regularly reviews the applied limits, adjusting them during the collaboration, and also offers the customer the opportunity to set a suitable limit below or above the default values set by the Institution, providing the possibility of limit change only after individual communication with an Institution employee, except in cases where the payment limit is increased to the level set by the Institution and therefore communication with an Institution employee is not mandatory, or in cases where the payment limit is increased insignificantly. In cases where an Institution's employee is not involved in increasing the payment limit, the Institution ensures that strong customer authentication is performed before increasing the payment limit;

5.1.3. the Institution applies transaction monitoring across all electronic payment channels where its customer uses a specific payment instrument, such as an ATM, ensuring integrated monitoring of transactions associated with the payment instrument;

5.1.4. when issuing a new payment card to a customer, the Institution assesses whether the customer requires the card for cross-border and e-commerce transactions. This prevents newly issued payment cards from being enabled for such payments by default and ensures that activation aligns with the customer's actual needs, considering the Institution's technological capabilities.

5.2. Cancellation of a payment order after its execution:

5.2.1. if a payment has been executed and the Institution has reasonable suspicions of financial fraud, it contacts the customer to obtain consent for notifying the recipient's Institution about the suspected fraud and requesting payment cancellation. The Institution informs the customer about the actions taken, the associated timelines, and the potential consequences in case the payment is cancelled or cannot be cancelled. The Institution does not communicate with the customer in cases where the Institution has reasonable suspicions that the customer's payment account is being used for the transfer of defrauded financial funds, including cases where the customer may be a money mule;

5.2.2. when a payment identified as financial fraud has been made using a payment instrument (a payment card or a digital wallet linked to a card), the Institution contacts the customer regarding the suspected fraud case and provides information on the payment cancellation procedure and the status of the reserved payment.

5.3. The Institution ensures that information regarding the significance of a payment card transaction's reservation status is communicated in plain language and is easily accessible and understandable to customers, including those without specialised knowledge in law or financial services.

6. Assessment of Payment Authorisation and Gross Negligence

6.1. The Institution establishes an internal procedure for decision-making on compensation of customer losses incurred in cases of financial fraud. The decision to compensate losses is based on an evaluation of the customer's actions in the fraudulent transaction, including their role in authorising the transaction and their ability to detect the fraud before its execution.

6.2. When assessing the customer's claim for compensation of losses incurred as a result of financial fraud, the Institution does not limit its assessment (decision) to merely providing a general explanation that the transaction was authorised, including through the use of strong customer authentication. The Institution also states in its assessment (decision):

6.2.1. the actual circumstances of the transaction, including the type of transaction (card transaction, credit transfer) and the information known to the Institution about the parties involved in the transaction;

6.2.2. information on the authentications used in the transaction (for identification of the person) and authorisations (for confirmation of the transaction), including strong customer authentication and the devices used for authentication and authorisation;

6.2.3. a general explanation of the circumstances known to the Institution or derived from the customer's application, which serve as the basis for identifying the customer's gross negligence, including failure to fulfil obligations stipulated in standard contracts, that lead to a case of fraud;

6.2.4. if applicable to the circumstances of the particular case, i.e. the customer denies having authorised the transaction with strong customer authentication, an explanation of the actual circumstances, including the actions taken by the customer that allowed third parties to gain access to the customer's authentication or authorisation tools or install the internet banking application on third-party devices, suggesting gross negligence, including non-compliance with the obligations stipulated in standard contracts, that lead to a case of fraud.

6.3. When assessing the customer's actions in relation to transaction authorisation, the Institution evaluates whether there are indications of gross negligence, such as:

6.3.1. the customer has completed strong authentication without reviewing the action to be performed (e.g. PIN1 for internet banking access or PIN2 for payment authorisation), on the condition that, before entering PIN2, the Institution has provided information that clearly specifies the payment recipient and amount;

6.3.2. the customer has not taken into account the information provided by the Institution, addressed to the customer and delivered through individual channels, regarding specific developments in the area of fraud;

6.3.3. the customer has given easy access to the payment card PIN by storing it alongside the payment card or writing it on the payment card;

6.3.4. the customer has failed to inform the Institution about any other suspicious transactions that have already occurred with the specific payment instrument or account;

6.3.5. the customer has fallen victim to fraud multiple times in identical or similar financial fraud cases;

6.3.6. in communication with third parties, the customer has shared payment instrument details, handed over the payment instruments themselves, or provided information enabling third parties to assume the customer's digital identity or gain access to internet banking, including installing the internet banking app on a third-party smart device.

7. Information Access Requirements

7.1. The Institution ensures that customers have easy access to detailed information about the complaint review process, the procedure for disputing transactions, and the steps to take if they suspect fraudulent activity. The Institution also indicates the available communication channels and process flow intended for these processes, clearly specifying the information the customer must provide in each respective case, and the potential outcomes of the process, as well as further actions if the customer's complaint or application cannot be resolved. The Institution urges customers to immediately report any suspicious activities they notice, including unauthorised transactions, unexpected account changes, or phishing attempts.

7.2. The Institution carries out the following initiatives to promote financial literacy:

7.2.1. through its own information dissemination tools (websites, social media, etc.) or by referring its customers to other publicly available and reliable sources of information, the Institution actively informs them about various detected fraud methods, unreliable or false website addresses and their characteristics, as well as actions to safeguard against potential fraud. Information must be timely and regularly updated;

7.2.2. the Institution informs its customers in a user-friendly and plain language on how to safely use payment instruments and payment services in an electronic environment and how to protect their payment instrument's personalised security data before starting to use the provided payment services. It is particularly important to specify in an appropriate manner, with examples, which actions in contractual relationships would constitute consent to payment. This information should be provided not only by providing information on the Institution's website, but also by using other effective communication channels and methods;

7.2.3. the Institution provides customer support on all aspects of service security, reporting anomalies and suspected fraud, ensuring they can promptly contact trained staff. If necessary, the Institution monitors the specific case. This service should be available at least during the Institution's working hours.