LIETUVOS BANKAS
EUROSISTEMA

FRAUD PREVENTION GUIDELINES

APPROVED
by Decision No V 2024/(1.160.E-9004)-441-16
of the Financial Market Supervision Committee
of 16 January 2024

CONTENT

INTRODUCTION

With a view to encouraging financial market participants to improve the management of financial fraud risk and increase the effectiveness of the applied prevention measures, as well as to improve compliance with the requirements set out in the legislation of the European Union and the Republic of Lithuania, the Bank of Lithuania has drawn up the Fraud Prevention Guidelines (hereinafter – the Guidelines).

The purpose of the Guidelines is to help financial market participants providing payment services to detect, assess and mitigate in a timely manner the risk of fraud, i.e. the risk that payment services provided by financial market participants to consumers may be used by persons with criminal intent for their own potentially fraudulent activities.

The Bank of Lithuania has not been authorised to officially interpret the laws and other legal acts; therefore, the general recommendations and examples of good practices provided in these Guidelines cannot be considered to represent an official interpretation of the applicable legal acts.

The list of recommendations and good practices provided in the Guidelines is not exhaustive, and the Guidelines will be periodically updated and improved with regard to the new trends of fraud and emerging issues in the payment services market. Financial market participants providing payment services may also apply other good practices than those indicated in the Guidelines, if they ensure the equivalent effectiveness of fraud prevention measures and compliance with the requirements set out in the legislation of the European Union and the Republic of Lithuania.

It is noteworthy that failure to comply with the applicable laws, regulations, and guidelines of the European Banking Authority and the recommendations and positions published by the Bank of Lithuania may result in the violation of the interests of consumers of payment services, damage to the reputation of financial market participants, and other losses.

The recommendations set out in these Guidelines on responsibilities and the indemnification of financial market participants providing payment services are aimed at providing greater protection to payment service users, who have limited ability to influence the fraud prevention process. Furthermore, financial market participants providing payment services have the possibility to develop their IT systems related to payment services so as to ensure maximum security commensurate with fraud risk, and payment service users have no impact on this process. It should also be noted that fraud prevention measures taken by financial market participants should not restrict the availability of services for conscientious payment service users.

The Guidelines are expected to improve the overall understanding of financial market participants on how fraud prevention measures should be implemented, to strengthen the powers and impact of the persons responsible for the implementation of these measures (fraud prevention officers) on the activities of financial market participants, and to promote the uniform and consistent implementation of fraud prevention measures by financial market participants.

CHAPTER I
RELATED LEGISLATION

1. Legal acts of the European Union:

1.1. Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC;

1.2. Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009;

1.3. Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions;

1.4. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC;

1.5. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC;

1.6. Joint Guidelines under Article 25 of Regulation (EU) 2015/847 on the measures payment service providers should take to detect missing or incomplete information on the payer or the payee, and the procedures they should put in place to manage a transfer of funds lacking the required information;

1.7. Commission Delegated Regulation (EU) 2018/389 of 27 No-

vember 2017, supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication;

1.8. The European Banking Authority's Guidelines of 1 March 2021 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ("The ML/PPTF Risk Factors Guidelines") under Articles 17 and 18(4) of Directive (EU) 2015/849 repealing and replacing Guidelines JC/2017/37;

1.9. The European Banking Authority's Guidelines of 31 March 2023 on policies and controls for the effective management of ML/TF risks when providing access to financial services (EBA/GL/2023/04);

2. Legislation of the Republic of Lithuania:

2.1. Republic of Lithuania Law on the Prevention of Money Laundering and Terrorist Financing;

2.2. Republic of Lithuania Law on Banks;

2.3. Republic of Lithuania Law on Credit Unions;

2.4. Republic of Lithuania Law on the Central Credit Union of Lithuania;

2.5. Republic of Lithuania Law on Electronic Money and Electronic Money Institutions;

2.6. Republic of Lithuania Law on Payment Institutions;

2.7. Republic of Lithuania Law on Payments;

2.8. Guidelines on the Prevention of Money Laundering and/or Terrorist Financing for Financial Market Participants approved by Resolution No 03-17 of the Board of the Bank of Lithuania of 12 February 2015 on the approval of the guidelines on the prevention of money laundering and/or terrorist financing for financial market participants;

2.9. Position of the Supervision Service of the Bank of Lithuania on the procedure for tracing a payment transaction in case of an incorrect unique identifier approved by Decision No 241-178 of 22 December 2014 of the Director of the Supervision Service of the Bank of Lithuania on the position of the Supervision Service of the Bank of Lithuania on the procedure for tracing a payment transaction in case of an incorrect unique identifier;

2.10. Guidelines for the Provision of Payment Services approved by Decision No V 2021/(34.3.E-3400)-419-30 of the Director of the Financial Market Supervision Service of 15 February 2021 on the approval of the guidelines for the provision of payment services.

CHAPTER II
SCOPE AND TARGET ENTITIES

3. These Guidelines shall apply to financial market participants supervised by the Bank of Lithuania which provide payment services (hereinafter – payment service providers, PSPs):

3.1. banks and foreign bank branches established in the Republic of Lithuania;

3.2. central credit unions;

3.3. credit unions;

3.4. electronic money institutions and branches of foreign electronic money institutions established in the Republic of Lithuania;

3.5. payment institutions and branches of foreign payment institutions established in the Republic of Lithuania.

4. The recommendations on the organisation of fraud risk management set out in Chapter IV of the Guidelines should be applied in a manner proportionate to the activities of PSPs, i.e. having regard to the size of PSPs, the volume of services provided, the payment methods used, customer categories, and the internal organisational structure. Furthermore, fraud risk management could be integrated into the internal organisational structures of PSPs in ways other than those set out in Chapter IV of the Guidelines (e.g. by delegating functions to compliance or risk management units or to the staff performing those functions), if PSPs are able to ensure the equivalent level of management of those risks and effective fraud prevention. The recommendations and good practices set forth in these Guidelines should be applied, taking into account of the readiness of PSPs and the proper integration of recommended measures and actions into the process of providing services to PSUs.

CHAPTER III
DEFINITIONS

5. For the purposes of the Guidelines:

5.1. **Fraud** means any act that involves the use of deception and/or other unlawful means to secure funds, such as:

5.1.1. misappropriation and/or other use of funds belonging to the payment service user (PSU) held in payment accounts of the PSU and/or otherwise in the possession of the PSU, as well as transactions concluded in the name of the PSU which have and/or may have financial consequences for the PSU, without the will and consent of the PSU (unauthorised payment transactions and/or transactions);

5.1.2. initiation and execution of payment transactions which are authorised with the PSU's own consent but after misleading the PSU as to the purpose and/or consequences of the payment transaction or other circumstances (authorised payment transactions);

5.2. **Employee responsible for fraud prevention** (hereinafter – Fraud Prevention Officer, FPO) means a person appointed by the PSP responsible for assessing the effectiveness of the payment transaction monitoring process and fraud risk management measures, and for applying prevention measures. The term "other staff performing the fraud prevention function" is used in the Guidelines when the provisions of the Guidelines apply not only to the FPO but also to other PSP staff;

5.3. **Fraud risk** means the risk that persons with criminal intent will use the payment services provided to users by PSPs for their own fraudulent activities;

5.4. **Risk-based approach** means an approach whereby PSPs identify, assess and understand their fraud risk and take proportionate measures to manage that risk;

5.5. **Managers of PSPs** means a person or persons who manage the activities of PSPs:
5.5.1. the head of administration;
5.5.2. members of the board;
5.5.3. members of the supervisory board;
5.6. **Phishing** means a social engineering technique in the digital environment that uses deception to obtain sensitive information such as usernames and passwords, bank account numbers, payment and credit card numbers, etc. by pretending to be a trustworthy natural or legal person;
5.7. **Vishing** means a type of fraud similar to digital phishing in which a call is made to obtain private personal data.

6. Other terms shall have meanings as defined in the legal acts governing the activities of a particular PSP.

CHAPTER IV
ORGANISATION OF FRAUD RISK MANAGEMENT

7. In the event of potential fraud, failure to comply with laws, regulations, and guidelines of the European Banking Authority and the recommendations and positions published by the Bank of Lithuania may result in damage to the interests of the PSUs, damage to the reputation of the PSPs, and other losses. Therefore, the managers of PSPs – being responsible for the effective and prudent management of PSPs (taking into account the provisions on internal control and risk assessment (management) approved by Resolution No 149 of 25 September 2008 of the Board of the Bank of Lithuania on the provisions for the organisation of internal control and risk assessment (management), the provisions on the Specification of the Requirements for the Management System and Protection of Received Funds of Electronic Money Institutions and Payment Institutions approved by Resolution No 247 of 30 December 2009 of the Board of the Bank of Lithuania on the requirements for the internal control and risk management and the protection of received funds for payment institutions, the requirements for risk assessment (management) set out in the Regulations on the Organisation of Internal Control and Risk Assessment (Management) of Credit Unions approved by Resolution No 03-25 of 6 February 2014 on the approval of the regulations on the organisation of internal control and risk assessment (management) of credit unions – should take responsibility for the proper organisation of the process of prevention of possible fraud. This includes, in particular, efforts to understand the actual fraud schemes faced by PSPs, trends in the related fraud indicators and ensuring that steps are taken to improve risk management and control systems and measures, thereby effectively preventing fraud.

8. Managers of PSPs should ensure that there is a designated FPO responsible for assessing the effectiveness of the payment transaction

monitoring process and fraud risk management measures and for applying prevention measures. Depending on its size, the scope of the services provided, the payment instruments used, the categories of customers and the internal organisational structure, a PSP may delegate individual tasks for the application of fraud risk management and prevention measures to other staff. [1]

9. At the same time, there should be an effective exchange of information between the FPO and other staff performing internal control functions (compliance, risk management, internal audit) and, where appropriate, external auditors.

10. In ensuring that sufficient human and other resources are allocated to fraud prevention, managers of PSPs should take into account individual circumstances (volume of payment services provided, number of customers, systems and technical tools used to monitor payment transactions, number of customer complaints about fraud, etc.) that may influence the fraud risk profile of PSPs. The FPO should be consulted before deciding on the allocation of resources for the fraud prevention function. Any decision to significantly reduce the resources allocated should be documented in writing, providingthe reasons for such decisions and providing an assessment of the consequences of such actions.

11. Where the scope of the PSP's activities is significantly expanded or a significant increase in the number of customer fraud complaints is observed, the PSP should ensure that the fraud prevention function is expanded as appropriate in line with changes in fraud risk. Managers of PSPs should regularly and at least once a year assess whether the number and competence of staff is sufficient to perform the fraud prevention function.

12. In addition to human resources, it is also recommended to allocate sufficient resources to advanced technological solutions (payment transaction monitoring, fraud detection tools, tools to determine the level of the PSU's risk of fraud), in line with market best practice, for fraud prevention.

1 In the three lines model of internal control used in international practice, the first line of internal control includes the operational controls exercised by a financial market participant's business units. The second line consists of internal controls (including fraud risk management function, controls over the reliability of financial and other information, controls over operational efficiency, etc.) carried out by the units responsible for compliance and risk management. The third line of internal control includes the control carried out by the internal audit function. Further information is provided in the Guidelines on Internal Governance of 2 July 2021 of the European Banking Authority (EBA/GL/2021/05).

13. The FPO and, where applicable, other fraud prevention staff should be provided with the necessary powers to carry out their duties effectively and should have access to all information relevant for the prevention of fraud and to all relevant databases and documents relating to payment services rendered by PSPs.

14. In order to ensure that the FPO would have the necessary powers (including sufficient competence and personal skills) to carry out their duties, the managers of PSPs should provide them with all the necessary conditions for the performance of these duties. A fraud prevention policy (or other internal document of the PSP) drawn up by the PSP, which, inter alia, clearly sets out the specific powers of the FPO, could also help to reinforce the powers of the FPO. The fraud prevention policy should be easily accessible and understandable to all employees of PSPs involved in the provision of payment services.

15. The FPO and, where applicable, other staff performing the fraud prevention function should be familiar with the laws, regulations, guidelines and positions of the European Banking Authority and the Bank of Lithuania regulating the activities of PSPs, as well as the typologies of fraudulent activities(including with regard to the direction of payment transactions and relevance by geographical regions and/or countries), to the extent necessary for the performance of their tasks. The FPO should have enhanced expertise, i.e. a sufficiently in-depth knowledge of payment transaction monitoring systems, technical tools, typologies of fraudulent activities and experience, and the competence to take responsibility for and ensure the effectiveness of fraud prevention.

16. Before appointing a person as an FPO, managers of PSPs should assess the candidate's qualifications. The FPO should have specific knowledge of the payment services provided by the PSP and the security measures in place, and sufficient professional experience to be able to assess the risk of fraud associated with the PSP's activities. The expertise required for different PSPs may vary due to the different nature of fraud risk. Therefore, the newly appointed FPO may require additional expertise in relation to the services provided by a particular PSP, potential fraud schemes, and the monitoring of operations and security measures in place, even if they have previously worked as an FPO for another PSP. The required professional experience may have been acquired in a position related to the execution of payment transactions or other internal control or regulatory functions.

17. Regular training and conditions for upgrading one's qualifications should be provided to the FPO and other fraud prevention staff to ensure that they do not lose competences.

18. It is considered to be good practice to conduct an assessment (self-assessment) of the effectiveness of the PSP's fraud prevention process at least once per calendar year. The assessment should take into account internal and external factors that may influence the statistical indicators of fraud cases. It is also recommended that an assessment of the compliance of fraud risk management with the organisational requirements, the effectiveness of risk management procedures, the achievement of fraud prevention objectives for the FPO and, where applicable, the performance of other staff performing fraud prevention functions is undertaken. The results of the assessment could be made public (paragraph 97 of the Guidelines) as a justification for the application of good fraud prevention practices and, where appropriate, provided to the Bank of Lithuania. Examples of self-assessment checklists are provided in Annex 1.

CHAPTER V
FRAUD RISK MANAGEMENT

1. Fraud risk assessment

19. With a view to ensuring that the resources for the fraud prevention function are efficiently allocated, PSPs should ensure that fraud risk assessments are carried out on a regular basis – at least once per year. The fraud risk assessment should be carried out in order to identify the main aspects and extent of the prevention of fraudulent activity, such as: whether the process of identification, collection and verification of PSUs is properly organised; whether profiles of potential fraudsters have been developed, typologies of their activities have been identified and the criteria for the identification of such activities have been appropriately selected; and whether the rules for the monitoring of payment transactions are properly applied and updated in light of the results of the previous assessment and their findings.

20. Based on the fraud risk assessment, fraud prevention objectives should be set and a fraud risk monitoring programme (or other appropriate document/plan) should be developed to manage the risks identified following the assessment. To ensure that any new aspect of risk (e.g. due to new fraud typologies, new applicable regulation, use of new service delivery channels/technologies, new customer groups, etc.) is taken into account, it is recommended to review the identified risks on a regular basis, as well as on an ad hoc basis whenever necessary.

21. The tools and methods used in the performance of the fraud risk management function, as well as the scope of the monitoring programme, the areas of controls and the frequency of monitoring (which may be periodic, ad hoc and/or continuous), should be determined by a risk-based approach.

22. The fraud risk monitoring programme (or other relevant document/plan) should reflect changes in the risk profile of the PSP that may arise, for example, due to significant events such as changes in information technology systems, the launch of new payment products/services, etc. The fraud risk monitoring programme (or other relevant document/plan) should also include the monitoring of the implementation and effectiveness of any actions taken by the PSP in response to identified fraud incidents.

23. The fraud risk assessment should take into account the requirements set out in the laws and regulations governing the activities of PSPs, as well as in legislation and/or related legislation aimed at fraud prevention, the guidelines and positions of the European Banking Authority and the Bank of Lithuania, as well as the internal policies, procedures, systems and controls implemented by PSPs. The assessment should also take into account, where applicable, the findings of an internal or external audit.

24. The FPO should also be involved in the monitoring of the procedure for dealing with complaints of PSUs possible fraud . Complaints received should be considered as an important source of information for the monitoring of fraud risk. The FPO should be given access to all PSU complaints received.

2. Fraud risk assessment reports

25. PSPs should ensure that written fraud risk assessment reports are prepared and provided to managers of PSPs on a regular basis, at a frequency determined by the PSP, after assessing the need and relevance of the updated information provided. These reports should contain information on the overall level of fraud risk, the preventive measures in place and their effectiveness, as well as the measures taken or to be taken to address the shortcomings identified in the assessment

and other material information. Material irregularities or shortcomings detected in the course of the fraud prevention function should be immediately reported by the FPO to the managers of the PSP.

26. It is recommended that fraud risk assessment reports contain information relevant to each PSP, if available (in the possession of the PSP):

26.1. an overview of the fraud risk faced by the PSP, including information on new types of fraudulent activity identified and any changes in the risk assessment of the company;

26.2. information on changes during the reporting period in relevant legislation and other requirements governing the PSP's activities that may have an impact on fraud prevention and their impact on the PSP;

26.3. an overview of the effectiveness of the transaction monitoring systems and fraud prevention measures in place;

26.4. information on the adequacy of staffing and IT resources in relation to changes in the level of fraud risk;

26.5. relevant information on the individual business relationship with the PSU, such as:

26.5.1. the number and nature of new business relationships;

26.5.2. the number and nature of business relationships that have been terminated as a result of fraud;

26.6. the number of warnings, complaints, and enquiries regarding fraud:

26.6.1. details of the number of fraud cases (by typologies of fraudulent activity, units, amounts);

26.6.2. information on the number of recoveries made to affected PSUs in cooperation with the PSPs that provided services to the fraudsters;

26.7. details of the losses suffered by PSPs and PSUs as a result of the fraud and the reasons for them.

3. Effectiveness of the payment transaction monitoring process

27. New fraud threats arise from rapid digitisation, social engineering and the use of new products for criminal purposes. As fraud schemes become more and more sophisticated, PSPs are recommended to

implement appropriate technological and organisational measures to increase the effectiveness of the payment transaction monitoring process and the proportion of fraud cases prevented.

28. In order to take advantage of the possibilities of monitoring the actions of PSUs before the initiation of a payment transaction, PSPs are recommended to implement technological solutions that would allow unusual customer behaviour to be detected. Technological solutions using historical data would help to configure specific segments of PSUs with higher fraud rates and identify changes in their behaviour.

29. Where a remote payment transaction is initiated, PSPs should apply the strong customer authentication procedure provided for by Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (hereinafter – the SCA Regulation) in order to ensure that each payment transaction is dynamically linked to a specific amount and a specific payee. The dynamic linking of the payment transaction to the payee and the amount should also be reflected in the window of the authentication tool used, where technologically feasible by the capabilities of the authentication tool, prior to the validation of the payment transaction by the PSU using PIN codes.

30. When implementing payment transaction monitoring mechanisms, PSPs are recommended to assign appropriate risk scores to payment transactions or to apply equivalent alternative solutions to group payment transactions according to the identified risk levels and to select appropriate control procedures and risk mitigation measures for each level. Such measures could include, for example, suspension or denial of the execution of a payment transaction, contacting the PSU, non-application of the exemption from the strong customer authentication rule specified in Chapter III of the SCA Regulation, or referring a payment transaction to the relevant competent criminal investigative authority (the police, the FCIS). Upon identification of a payment transaction with a high risk level determined by the PSP, risk mitigation measures should be applied immediately in relation to that payment transaction, taking into account the specificities of the execution of the payment transaction concerned.

31. A good practice would be to establish a mechanism for monitoring payment transactions in such a way as to take into account the interoperability between different risk levels and risk-based factors.

32. In addition to the risk-based factors identified in the SCA Regulation, it is recommended that the payment transaction monitoring process should also take into account factors that could help to more quickly identify any unusual behaviour of PSUs and increase the effectiveness of monitoring, such as:

32.1. the installation of a new payment instrument (e.g. a mobile banking application) on a device unknown to a PSU;
32.2. unusual payment transactions;
32.3. the use of a payment instrument and/or access device in a different way than before;
32.4. the location in which payment orders are provided;
32.5. the use of IT tools and IP addresses which were used in previous cases of abuse and which were known to a PSP;
32.6. details of previously identified fraud cases;
32.7. the location and network details of the device or software used for access;
32.8. indications of the presence of malware at any stage of the authentication process;
32.9. inconsistency in the number of devices or software used for access with the PSU's profile;
32.10. potential business relationships between the payer and the payee;
32.11. a report of suspected fraud, etc., by any natural person (PSU).

The fraud scenarios used by the PSP should be periodically updated, with regard to the latest known fraud trends.

33. It is recommended that the PSP adopts performance indicators for the operation monitoring mechanisms. Taking advantage of the exemption indicated in Article 18 of the SCA Regulation, the PSP should additionally monitor the fraud indicators and their values. Information on these indicators should be included in the fraud risk assessment report referred to in paragraph 26 of the Guidelines, and in case of urgent circumstances, the FPO should provide the relevant information to the managers of PSPs without delay.

34. PSPs are recommended to use the payment transaction monitoring tools that ensure real-time monitoring of transactions, as well as provide the ability to identify unusual customer-specific transactions

and to adapt new rules or scenarios. In addition, PSPs could also use retrospective monitoring tools to review PSU activities over a longer period of time in order to identify any signs of potential fraud. The findings of retrospective monitoring should also be used to develop new fraud detection and prevention tools. PSPs should allocate sufficient financial and information technology resources to enable the application of advanced transaction monitoring solutions, the inclusion of more and varied monitoring criteria and the introduction of advanced technological solutions (e.g. in the area of customer profiling). Periodic assessment of the effectiveness of the payment transaction monitoring mechanisms in place is important to determine whether they are able to detect potential fraud in a timely manner, to investigate the reasons for ineffective monitoring, to use the information from the analysis and internal investigations to develop new monitoring rules, and to proactively introduce additional technological solutions in order to prevent potential fraud.

35. The technological solutions and/or modules applied to the monitoring of payment transactions should not be restricted only to the tools needed to manage the risk of money laundering and terrorist financing. Instead, it is recommended to supplement these systems with such solutions and/or modules that would reflect the aspects of fraud prevention more effectively (e.g. the inclusion of payment transaction indicators into additional monitoring scenarios).

36. By pentesting the security measures in place for payment transactions (i.e. penetration tests to check whether the PSU authentication procedure is likely to be penetrated by malware), the processes of PSU authentication procedures should be tested at least once per year and whenever there is a change of infrastructure, to ensure that they continue to be relevant and effective in line with the level of fraud risk faced by the PSP.

37. In the event that tasks related to the monitoring of payment transactions, including the management of alerts generated by IT systems, are carried out by employees working in different units of PSPs, PSPs should ensure that these units (staff members) coordinate their activities with the FPO and act in conjunction with the FPO in order to ensure the most effective prevention of fraud cases.

38. Payment transaction security measures applied by PSPs should be independently audited every three years and, in cases where the PSP makes use of the exemption referred to in Article 18 of the SCA Regu-

lation, the methodology, model and fraud indicators applied should be independently audited at least once per year.

4. Handling complaints of possible fraud

39. PSPs should carefully monitor and analyse any incoming complaints of potential fraud, as well as cases in which PSUs using its services are suspected of fraud and any complaints or requests to provide information on them are received from correspondent banks, other financial institutions and/or law enforcement or judicial authorities.

40. Complaints received about possible fraud by a PSU using the services of a PSP should not be dealt with in a merely formal way, but in a thorough and detailed manner. They might involve, for example:

40.1. a more detailed review of the operations and activities of the PSU in question, in particular where at least one complaint or piece of information from other authorities has been received in relation to that PSU;

40.2. requesting additional documentation and information on the activities of the PSU concerned;

40.3. regular searches of public systems or public sources for information on the PSU concerned and analysis of such information;

40.4. assessing the transactions and information provided by PSUs through the prism of the validity and logic of the economic activity (i.e. whether the activities of PSUs are in line with the normal activities or activities that are typical of the economic activities specified by the PSU, etc.);

40.5. paying attention to whether, in the case of payments received by the PSU from other persons, such persons indicate a different name (in the beneficiary's field) than that of the PSU (a higher number of such cases may indicate misleading information as to the final beneficiary of the funds);

40.6. a more detailed assessment when different geographical information is provided at the time of identification of the PSU (e.g. different countries of registration, actual activity, telephone number, nationality and residence of the beneficiary or representatives as indicated by the PSU);

40.7. assessing the date of establishment of the legal entity of the

PSU, the period of active operation, the number of employees and the official seat/address, the place of operation, and the nature of the activity;

40.8. analysing, where possible, the traffic on the website of the PSU's legal entity (e.g. checking for signs of fraudulent traffic generation), as well as an assessment of the website itself (e.g. whether it is a fake copy of a legitimate website);

40.9. taking due account of the beneficiaries and representatives of PSUs, the possible affiliations of these persons (e.g. the PSU states that it will carry out consultancy activities, but links to Forex activities are found), the nationalities of the beneficiaries or the representatives, which are from third countries, including countries associated with a higher risk of fraud (e.g. boiler room fraud typologies), and other negative information;

40.10. regular verification of the activity of licences held by PSUs;

40.11. a comprehensive IP address check, assessing whether the geographical location of the IP address coincides with the location of the PSU's business or headquarters;

40.12. checking that the PSU is not included in the lists of entities providing illegal services (e.g. the Bank of Lithuania's list of entities not entitled to provide financial services in Lithuania,[2] the list of illegal operators published by the Gaming Control Authority,[3] the list of illegal investment service providers of the International Organization of Securities Commissions (IOSCO),[4] as well as the public lists published by other national supervisory authorities, such as the financial market supervisory authorities of the United Kingdom,[5] Italy, and Switzerland[6]).

41. Detailed analysis of the complaints received could help PSPs to develop profiles of potential fraudsters, typologies of their activities and criteria for identifying such activities, which could be used as a basis for improving the monitoring rules.

42. In order to increase the effectiveness of the fraud prevention measures in place, the PSP should continuously monitor the statistical information on the number of complaints it receives, comparing the number of complaints with the total available PSU database.

2 https://www.lb.lt/lt/subjektu-sarasas
3 https://lpt.lrv.lt/lt/nelegalios-losimu-veiklos-vykdytojai/nelegalios-losimu-veiklos-vykdytoju-sarasas
4 https://www.iosco.org/investor_protection/?subsection=investor_alerts_portal
5 https://www.consob.it/web/consob-and-its-activities/warnings?viewId=ultime_com_tutela
6 https://www.finma.ch/en/finma-public/warnliste/

43. Information gathered during the investigation of fraud complaints should also be included in the risk score when assessing the PSU's individual risk of fraud.

5. Information (documents) provided by PSUs

44. When requesting information from a PSU for fraud risk management purposes (due to possible fraud by a PSU using the PSP's services), the PSP should explain in more detail the specifics of the documents and/or information requested, i.e. what documents are required (e.g. the content and format of the documents, what information they must contain, who issues them, etc.). The amount and nature of the information requested from the PSU may vary from case to case (taking into account the totality of the circumstances and the possible typologies of fraud), but the information requested should be such as is necessary to ensure that the risk of fraud is properly assessed and managed.

45. When establishing policies and procedures for fraud risk assessment and management, PSPs should take into account the guidance of competent authorities on monitoring business relationships and reporting suspicious activity and should consider the totality of the circumstances in a holistic manner – for example, whether the requested information will have a material impact on the assessment of the risks associated with a particular business relationship and/or payment transaction and will help to appropriately manage the existing risks, as well as whether it is within the PSU's objective capability to provide the requested information, and if there are no other measures to manage the risks involved.

46. It is recommended to maintain regular contact with PSUs by providing a proper explanation of what information/documents should be provided and why. If the PSU is unable to provide specific documents in the acceptable forms , arrangements can be made to provide information equivalent to the requested data. Such explanations would help the PSU to understand what information is necessary for the business relationship and avoid the inaction (delays in providing documents) by the PSUs due to potentially incomprehensible requests.

47. Additional communication tools to which PSUs would be directed to provide information to support the business relationship (e.g. relevant digital and/or physical leaflets (one-pagers), Frequently Asked Questions (FAQs) on the PSP's website, and/or a dedicated section on this topic on the PSP's website) would help to ensure a more efficient and less costly process of collecting the appropriate data. PSPs should also inform PSUs about available/accessible data sources to avoid situations in which PSUs order the requested information/documents from inappropriate (and, in some cases, also paid) sources.

48. All available secure communication channels capable of ensuring rapid information and feedback, i.e. not only the email and/or physical address provided by the PSU, but also the telephone number or other communication channel specified for the PSU's communication. Feedback is particularly important once the PSU has submitted the requested information/documents, and the PSU should therefore be informed immediately of the status of the submission/assessment of information/documents. The PSP should inform the PSU of the length and progress of the process when reviewing and assessing the information received from the PSU. Various technological solutions can be used to maintain, speed up and facilitate communication between the PSP and the PSU (e.g. virtual chatbots, etc.).

6. Payment order cancellation procedures

49. Effective fraud prevention can only be achieved through appropriate action and prevention measures throughout the payment transaction process. Active action not only by the PSP providing services to the PSU (payer) to stop the payment as potentially fraudulent (i.e. to cancel it), but also by all other financial institutions involved in the payment transaction process (e.g. payment initiation service providers, the payee's PSP, etc.) to react promptly and cooperate is essential.

50. In order to ensure the adequate security of both the funds of PSUs and the provision of payment services themselves, the PSPs are recommended:

50.1. to ensure the availability of the PSP (both to PSUs and to other financial institutions involved in the process of a particular payment transaction) outside working hours, including week-

ends, by allowing the PSU to inform the PSP of possible fraudulent activity, to block not only the payment card but also access to the payment account, to initiate the procedure of revocation of the payment order or of the consent to initiate or execute a payment transaction (where the consent to initiate or execute the payment transaction has been given to the payment initiation service provider or to the payee) and to perform other similar actions;

50.2. to make PSUs aware of the means and steps to report fraud and/or to request the cancellation of a disputed payment transaction/recovery of the amount of such a transaction in the framework contract and/or in other ways that are easily accessible and clearly visible to PSUs;

50.3. in order to ensure that the PSU is able to contact the PSP in a timely manner, to establish a separate channel and/or a clear and fast way for the PSU to contact the PSP in case of fraud and/or to request the revocation of a disputed payment transaction (e.g. a separate telephone number, call function, etc.);

50.4. after the PSU has contacted the PSP in the manner referred to in paragraph 50.3 of the Guidelines, to ensure that the payee's PSP and/or the other financial institution involved in the execution of the payment (depending on the type of payment transaction) is contacted immediately, without waiting for the business day, informing them about the request received from the PSU and that the payee's PSP and/or the other financial institution involved in the execution of the payment responds to the message of the payer's PSP as quickly as possible;

50.5. to actively cooperate with other financial institutions involved in the payment transaction process, including the exchange of best practices, prompt action to stop/cancel the payment transaction, and reasonable efforts to recover the funds of the PSU;

50.6. not to limit oneself to formal processes only and to look for other (non-standard) possible ways to help PSUs recover their funds (i.e. immediately informing stakeholders through all possible channels of information provided by the PSU regarding a potentially fraudulent payment, despite the fact that the time limit for cancelling a payment order or consent has expired, etc.).

51. When informing PSUs about the possibilities to cancel payment orders (including consent given to initiate or execute a payment

transaction) and the applicable cancellation procedures, particular attention should be paid to enhancing the functionality of the presentation of this information (e.g. such information could be made available when logged into e-banking or in the payment order initiation window, and explanations could also be given in the cancellation window of the payment transaction, etc.). The PSU should also be personally informed about the stage of the procedures for revocation of a payment transaction and the actions taken or planned. General information on the payment revocation procedures and a clear sequence of the PSP's actions should also be made available on the PSP's website, in a clearly visible place.

52. PSUs often lack information on the part of the execution process of card-initiated payment transactions, where the funds of such payment transactions are displayed as 'reserved' in the systems of PSPs (PSUs, seeing the status of an ongoing payment transaction as 'reserved', usually have the expectation that the payment can still be stopped/cancelled, despite the fact that the balance of funds displayed in the system has already decreased). Given that a proper understanding of the status of the term of 'reserved funds' is particularly important in the case of fraud in relation to PSU, it would be considered good practice for the PSP:

52.1. to provide a clear and understandable explanation of the term of 'reserved funds', including information on whether these funds can be recovered in a more visible place (e.g. in the e-banking system by the specific payment transaction, on a website, or in any other easily visible place);

52.2. to explain how payment transactions made by payment cards are executed, i.e. when such payments are deemed to have been made (i.e. confirmed and/or executed) and when and what action the PSU could take to suspend/cancel a payment transaction made by payment card;

52.3. to clarify when and in what procedures the cancellation of a funds reservation is possible, when the PSP is not able to cancel the funds reservation and/or suspend/cancel a card payment transaction, how and within what time limits to apply, and whether there is a charge for such procedures.

53. PSPs should respond promptly to PSU enquiries and requests:

53.1. regarding the inconsistency of the payee's details in the payment order with the information available to the PSP about the payee specified in the payment order;

53.2. regarding the revocation of a payment order or consent (e.g. without setting additional time limits for such requests), allowing PSUs to submit such requests in a prioritized order;

53.3. clarifying the purpose of the PSU's request (to cancel a payment transaction) and providing relevant information to enable the PSU to decide on further action, etc.

54. Taking due account of the speed of fraudulent actions during the execution of payment transactions, PSPs should organise the process of handling fraudulent appeals received from PSUs so that the number of actions to be performed by PSUs is optimal, or the referrals queue is as short as possible (e.g. the action "if you think you have encountered fraud" is moved to "click on 1", rather than "click on 5, then on 8, then on 2", etc.).

55. The payee's PSP and the PSU (the payee) have the right to agree, insofar as it does not contradict the mandatory legal requirements, on the method of obtaining the PSU's (payee's) prior consent to debit the amount of the payment transaction credited to their payment account when/in case the payer submits a request to refund the amount of the payment transaction its PSP (hereinafter – the Payer's Request). Such a Payer's Request should be based on the fact that the disputed payment transaction was executed for and/or because of possible fraud. The agreement between the payee's PSP and the PSU (of the payee) on the prior consent of the PSU (the payee) to debit the amount of the payment transaction credited to their payment account in the cases referred to in this paragraph should be set out in a clear and transparent manner in the terms and conditions of the provision of payment services of the payee's PSP and/or in the framework contract for payment services.

56. The payer's PSP should, upon receipt of the Payer's Request, make reasonable efforts to promptly investigate the circumstances of the execution of the disputed payment transaction and to gather sufficient evidence to substantiate the fact stated by the PSU (the payer) that the disputed payment transaction may have been executed fraudulently and/or as a result of fraud.

57. The payee's PSP should, upon notification by the payer's PSP that it has received the Payer's Request:

57.1. obtain assurance that the Payer's Request submitted by the payer's PSP is based on the fact that the funds have been received by way of fraud as defined in paragraph 5.1 of the Guidelines;

57.2. take measures to collect sufficient data to assess the origin and source of the funds received, the basis and purpose of the payment transactions and/or data to confirm or deny the fraudulent circumstance, and contact its PSU (the payee) in order to investigate the circumstances referred to in the Payer's Request (unless the PSP itself has collected sufficient data to confirm the fraudulent circumstance);

57.3. seek the consent of the PSU (the payee), even if the PSU has given its prior consent, for the repayment of funds to the payer;

57.4. take a decision on the write-off of funds only after the steps referred to in paragraphs 57.2 and 57.3 of the Guidelines have been completed;

57.5. inform the payer's PSP and their PSU (the payee) of the decision referred to in paragraph 57.4 of the Guidelines.

58. Complaints by PSUs (the payees) against the reasonableness of a decision referred to in paragraph 57.4 of the Guidelines shall be dealt with in accordance with the general complaints handling procedure.

59. If it is established that the decision referred to in paragraph 57.4 of the Guidelines has been taken unreasonably, or if new circumstances arise which cast doubt on the reasonableness of the decision of the PSP, the payee's PSP shall be liable to compensate for the losses incurred by the PSU (the payee) as a result of this decision. The terms and conditions governing the liability of the payee's PSP to compensate the PSU (the payee) for losses resulting from an unjustified decision to debit should be included in the terms and conditions of the payee's PSP for the provision of payment services and/or the framework contract for payment services.

60. The possibility for the parties to agree on the method of obtaining the prior consent of the PSU (the payee) to debit their payment account for the amounts of the payment transactions credited to their payment account does not exclude the PSP's (both the payer's and the payee's) obligation to duly comply with the requirements of other legal acts, including, but not limited to, those relating to the monitoring of the transactions and the PSP's obligation to refund the amount of the payment transaction that has not been authorised by the PSU as well as the requirements relating to, but not limited to, those applicable in the area of the prevention of money laundering, etc.

CHAPTER VI
ENHANCING THE RESILIENCE OF PSUs AGAINST CYBER FRAUD

61. PSPs should develop and implement processes to raise awareness among PSUs of the security risks associated with payment services.

62. Using information dissemination tools (websites, social networks, etc.), PSPs should inform PSUs about fraud techniques, the addresses of untrustworthy or fake websites, signs, and ways to protect themselves from potential fraud or refer them to other publicly available and reliable sources of such information (e.g. the website of the Bank of Lithuania and/or the Association of Lithuanian Banks, etc.). This information should be up-to-date and regularly updated.

63. The PSP should provide information to PSUs in a language that is friendly and understandable to the PSUs, by aligning the provisions set out in the terms and conditions of the payment service or the framework contract with the information on the PSP's website (i.e. by including the essential information in the general conditions and by providing up-to-date links to relevant detailed explanations on the website) concerning:

63.1. how to use payment instruments and payment services securely in the electronic space and how to protect the personalised security features of their payment instruments even before starting to use the payment services provided;

63.2. what obligations the PSUs assume in the framework contract;

63.3. which actions of the PSUs in the contractual relationship would be considered to represent consent to the payment

transaction (in particular where different types of payment transactions are subject to different authorisation methods/ requirements, e.g. for wire transfers, card payments, payments via Apple Pay and/or other digital wallets, etc.).

64. The PSP should clarify to the PSUs that when informing by electronic means about changes in the provision of payment services (e.g. an updated e-banking system), it should not send online links to the PSU's internet bank together with a request to log in using personalised security features of the payment instruments in the notification (in the emails it is advisable to only provide links to the publicly available information on the changes in the terms and conditions for the provision of the services, i.e. "Read more", etc.).

65. PSPs should also adequately inform PSUs of all possible cases where the PSU may be asked to provide certain confidential personal information (e.g. personal identification number, ID number), but not personalised security features of payment instruments, when communicating by means of a communication (e.g. if a PSU seeks to increase the limits of their transactions by filling in the relevant request via e-banking, the PSP may contact the PSU and ask the PSU to provide the confidential information to check whether the PSU has actually submitted the request themselves).

66. PSPs should provide assistance to PSUs in all matters and respond to requests for assistance and notifications, queries about non-typical situations or problems related to the security aspects of payment services. Once a PSU becomes a victim of fraud, the PSP should contact the PSU and provide the necessary information for further action. The assistance and advice provided should be updated in light of new threats and perceived vulnerabilities, and PSUs should be informed about changes they may encounter as a result of the new features of the provision of payment services.

67. It would be good practice to have a separate channel (e.g. a phone number, a separate priority call function button, an active section entitled "Have you encountered fraud? Report and/or ask", with redirection and other relevant information on the website homepage, etc.), which would enable a fraud victim to contact the PSP as quickly as possible and report the fraud.

68. According to the assessment of the Bank of Lithuania, misuse of the authentication tool – not based on correct knowledge and skills – in the provision of payment services (in relations with PSPs), should be classified as a risk factor related to the provision of payment services, the ignorance and neglect of which may lead to unauthorised payment transactions due to fraud. Therefore, the authentication tools offered and/or allowed for use by PSPs should not only be secure for the PSUs that use them in their contractual relationship with the PSP, but should also be clear: the conditions for their use should be made transparent and precise, and the legal consequences of the actions carried out with the authentication tool chosen by the PSU should be specified, such as by providing a clear understanding of the legal implications of entering PIN codes.

69. Updates and changes to the terms and conditions of payment services, changes to the procedures for the provision of payment services by PSPs, and the introduction of new services that require and use an authentication tool in the process, should be tested prior to the entry into force of the respective updates/changes or the launch of the new services, and, from the perspective of the secure use of this authentication tool, the potential risks of fraud should be assessed and the ways to eliminate these risks should be considered and adapted.

70. Before offering a particular authentication tool to its PSUs, the PSP should make sure that this authentication tool is suitable for the PSU in question: even before choosing and using a particular authentication tool, the PSU should be made aware of the main features, including the security risks, of using this authentication tool in its relationship with the PSP and in the provision of payment services. A PSU should not be offered only one specific authentication tool, but all the options available to choose the authentication tool best suited to the needs of the particular PSU.

71. PSPs should aim to make use, where technologically feasible, of the capabilities (functionalities of the authentication tool) provided by the issuer of the authentication tool in order to inform the PSU as accurately and completely as possible about the nature and purpose of the action for which the specific PIN code of the respective authentication tool is requested. Where technologically feasible, it is good practice for PSPs to authenticate payment transactions initiated through the payee by requiring that at least one of the notifica-

tion windows of the authentication tool requesting the entering of the PIN1 code of such a device, which would confirm the payment transaction by card, would indicate the meaning of entering this PIN code – i.e. the details of the payment transaction for which consent will be given by entering the PIN1 code – the name of the payee of the funds, the amount of the payment transaction.

72. The PSP should pay sufficient attention to the awareness of its PSUs by increasing their knowledge of the secure use of payment instruments, including the chosen authentication tool used in the relationship with the PSP, and should regularly update, keep up-to-date and communicate this information to their PSUs. Such information should include, inter alia, guidance on the choice of passwords, the protection of confidential data, ways to protect against fraud when using the chosen authentication tool, etc.

73. The familiarisation of the PSU with the procedures for the use of the authentication tool should not only be formal, i.e. providing the PSU with information in clear and understandable language on the main features of the use of the authentication tool and the associated security risks, but also allowing the PSU themselves to assess their readiness to use the chosen authentication tool and its suitability for the needs of the PSU concerned. Therefore, it is good practice to offer PSUs the opportunity to assess their knowledge on the appropriate and secure use of the authentication tool by means of an interactive, preferably digitally-delivered, small-scale test, when providing PSUs with access to essential information on the authentication tool of their choice. Such a test/questionnaire could test both the knowledge of the particular PSU on the essential conditions for the (secure) use of the authentication tool and the practical skills to use it.

74. In the event of a failure to pass a test developed by the PSP on the chosen authentication tool, the PSU could be offered to re-read the guidance on the safe use of this authentication tool, with additional attention paid to incorrect answers, and subsequently to re-perform the test. If the PSU fails to pass such a test several times, they could be directed to consult an appropriate specialist or to further familiarise themselves with the use of the chosen authentication tool. In such a case, the PSU should also be offered the possibility of choosing another authentication tool, and the security risks associated with using the authentication tool without adequate preparation should be explained.

CHAPTER VII
REIMBURSEMENT OF LOSSES

75. A fair and individual reimbursement process for disputed payment transactions due to fraud is an important part of both the provision of payment services and effective fraud prevention. Ensuring and enforcing the PSU's right to fair and individual reimbursement gives the PSP an incentive to take all necessary measures for effective fraud prevention to ensure that neither the PSU nor the PSP suffers any losses as a result of fraud. PSPs should ensure that the process of handling the complaints and requests of PSUs for disputed payment transactions complies with both the legal requirements and the judicial and extra-judicial practice for such disputes, and that it creates the preconditions for a thorough and reasoned assessment of each individual case.

76. Upon receipt of a complaint challenging the validation of a payment transaction, the PSP shall immediately, and no later than the end of the next working day following the receipt of the complaint, commence its examination. The time limit for the examination of said complaint may not exceed the maximum time limits for the examination of complaints filed by PSUs as laid down in the legislation. The time limits set out in the legislation and in the Guidelines shall also be respected in cases where the amount of the unauthorised (disputed) payment transaction must be refunded to the PSU immediately.

77. When a payment transaction is disputed by a PSU as having been executed by fraudsters and/or as a result of fraudulent activity (i.e. in cases where both the authentication procedures themselves (their proper execution) and other circumstances of the execution of the payment transaction are disputed), it should first be determined whether the

disputed payment transaction should be considered as an authorised payment transaction (a model chart for the recognition of a duly authenticated payment transaction can be found in Annex 2). It should be determined whether the disputed payment transaction:

77.1. was authorised in the manner in which the parties have agreed to authorise the submitted payment orders in the concluded agreement (the objective element);

77.2. was executed with the knowledge and consent of the PSU, i.e. whether there was a will on the part of the PSU to execute the payment transaction in question (the subjective element).

78. In the event that the PSU disputes the fact of authorisation of a payment transaction, it shall be the PSP that bears the burden of proving that such a payment transaction has been duly authorised in the form and manner agreed by the parties. In the event that the disputed payment transaction has been subject to a more secure authentication procedure, it is also important to establish the specific manner in which such a procedure was implemented and to gather and assess evidence that, in the specific case at issue, security measures were properly applied to ensure the confidentiality and integrity of the personalised security features of the PSU's payment instrument.

79. The mere fact that the use of a payment instrument issued by a PSP, including its personalised security features, has been recorded in the PSU's internal systems (e.g. the entry of PIN codes) is not necessarily sufficient proof that the PSU has authorised a payment transaction or acted fraudulently or has deliberately or with gross negligence failed to fulfil one or more of the obligations imposed on them in relation to the use of a payment instrument. Therefore, the PSP should also assess the following:

79.1. the possibility of misappropriation of the PSU's identity, i.e. whether the PSU's identity could have been misappropriated by a third party by intercepting and/or setting up a new authentication tool in the name of the PSU (installing a new account of an authentication tool (app, mobile signature, etc.) in the name of the PSU on the end-device controlled by a third party). For example, a payment transaction should be considered as unauthorised if it is established that, although it formally complies with the form and procedure agreed between the parties for giving consent to the payment transaction, it is actually confirmed by the creation of a new authentication account in the name of the PSU on another mobile device that

is not owned and used by the user but is controlled by third parties (fraudsters);

79.2. the possibility that the PSU's payment instrument or its personalised security features may have been intercepted, stolen or misappropriated by a third party. For this purpose, it should be assessed as to who initiated and/or provided the PSP with the data necessary to initiate and validate the payment transaction and by what means. That is to say, it is not only important to establish whether the disputed payment transaction was authorised in the form and manner agreed between the parties, but also whether the PSU themselves voluntarily consented to the disputed payment transaction. For this purpose, the payment transaction monitoring data, the circumstances of the execution of the disputed payment transaction as reported by the PSU, the data provided by the PSU in relation to the circumstances of the initiation and execution of the payment transaction, and any other data may be assessed;

79.3. any other circumstances that substantiate or deny the PSU's statement that they did not have the intention to initiate and/or authorise the disputed payment transaction. For example, it should be taken into account whether the documents governing the contractual relations between the parties and/or any other form available to the PSU have personally explained to the PSU the significance of the entry of the PIN codes of the authentication instrument used by the PSU in the process of execution of payment transactions and the possible consequences of their use for the PSU (i.e. what actions the PSU may perform using the relevant authentication instrument and what actions and in what cases the use of the authentication instrument and the entry of its PIN codes entail the relevant legal consequences).

80. A payment transaction, although formally authorised in the manner agreed between the parties, shall not necessarily be deemed to have been duly authorised by the PSU themselves if there is evidence of a lack of the payer's intent to execute the payment transaction (i.e. the payer's failure to express this intent, the influence of third parties, misleading the payer about the true meaning of their actions, the consequences of their actions, etc.). If there is sufficient objective evidence that the disputed payment transaction may have been initiated and authorised by the will and unlawful actions of third parties, i.e. the unlawful misappropriation of the PSU's payment instrument and/or its

personalised security features, as well as the substantial misleading of the PSU as to the circumstances of the payment transaction or the consequences of the actions required to authorise the payment transaction, the payment transaction could be considered as unauthorised (the subjective element of the authorisation of a payment transaction).

81. It would be good practice for the PSP to seek to ascertain all the circumstances of the execution of the disputed payment transaction and the related facts, which would enable the PSP to make a proper and reasonable assessment of both the circumstance of the authorisation of the disputed payment transaction and the PSU's own conduct, where the PSP determines that the disputed payment transaction should be considered as unauthorised, but that the execution of the payment transaction could have been due to the PSU's intent (bad faith) or gross negligence.

82. If the disputed payment transaction is declared as authorised, the issue of compensation for damages can be addressed on the general grounds of civil liability.

83. Upon becoming aware of an unauthorised payment transaction or upon declaring the disputed payment transaction as unauthorised, the issue of the reimbursement of the amount of the unauthorised payment transaction to the PSU should be settled in accordance with the procedure and within the time limits set out in Article 38 of the Law on Payments.

84. The PSP may be fully exempted from the obligation to reimburse the amount of the unauthorised payment transaction to the PSU only if the PSP has reasons to suspect the fraud of the PSU and notifies the Bank of Lithuania of these reasons and submits the supporting data in writing within the time limits set out in paragraph 83 of the Guidelines, as well as in cases where the PSP proves that the PSU has acted with intent in bad faith or with gross negligence. The notification to the Bank of Lithuania regarding the suspected fraud of a PSP should be submitted and the investigation of the circumstances related to the possible fraud of a PSU should be carried out in accordance with the procedure and within the time limits set out in the Rules Regarding Operational or Security Incident Reporting to the Bank of Lithuania approved by Resolution No 03-10 of 21 January 2019 of the Board of the Bank of Lithuania On the Approval of the Rules Regarding Operational

or Security Incident Reporting to the Bank of Lithuania and of Notification Templates.

85. In case the PSP has reasonable grounds to suspect the PSU's intent (dishonesty) and informs the Bank of Lithuania of these grounds and provides evidence to support them, the latter shall have the right to refuse to immediately reimburse the amount of the disputed payment transaction to the PSU by informing the PSU of the reasons for such a decision in writing, together with the evidence to support it, and specifying the procedure of handling complaints and/or disputes. Such a decision should be taken at the latest by the end of the business day following the day on which the PSP becomes aware or is informed of the payment transaction disputed by the PSU as being unauthorised. The submission of the notification of the suspected intent of the PSU to the Bank of Lithuania and the provision of information about it to the PSU shall not relieve the PSP from the obligation to conduct a thorough investigation of the payment transaction disputed by the PSU and to make a reasoned and evidence-based final decision on the request for the return of the funds of the disputed payment transaction to the PSU.

86. The liability of the PSU (full or partial) for unauthorised payment transactions is only possible in cases provided for by law. The PSP may be fully exempted from the obligation to reimburse the PSU for the amount of the unauthorised payment transaction only if they provide evidence of the PSU's dishonesty, intent or gross negligence.

87. Where the PSP does not require more secure authentication, the PSU shall not suffer any loss as a result of unauthorised payment transactions, even if the PSU has acted negligently or even grossly negligently, unless the PSP proves the PSU acted in bad faith. However, in cases where the PSP applies a more secure authentication procedure to the PSU's login to the internet bank and payment account, and the more secure authentication is not applied to the initiation of payment transactions made after the login, after taking advantage of the exception to the SCA Regulation referred to in Article 16, the issue of allocation of liability for unauthorised payment transactions, in the opinion of the Bank of Lithuania, could be resolved in accordance with the procedure laid down in paragraph 84 of the Guidelines.

88. Gross negligence, as well as intent or dishonesty, are circumstances of an evaluative nature; therefore, when deciding on a case-by-case basis on the recognition of the PSU's conduct as grossly negligent (dishonest, to be assessed as intent) and resulting in an unauthorised payment transaction or loss of a payment instrument, the PSP shall assess the totality of the individual, specific circumstances of the case, established by the PSP, which are known to the PSP, and which are supported by the evidence in the possession of the PSP, and/or the circumstances are not disputed by the parties.

89. The fact that PSUs breached their duty to adequately protect the confidentiality of the personalised security features of their payment instruments does not in itself imply that the conduct of PSUs was grossly negligent. The PSU shall only be liable for all losses resulting from unauthorised payment transactions if both of the following conditions are met:

89.1. the PSU fails to fulfil one or more of the obligations imposed on it by the Republic of Lithuania Law on Payments relating to the use of payment instruments and their personalised security features;

89.2. the PSU's actions are intentionally dishonest or committed with gross negligence.

90. In order to determine whether the behaviour of a particular PSU in relation to the execution of an unauthorised payment transaction can be considered as gross negligence, the totality of the circumstances should be assessed (examples of possible behaviour of a PSU as reckless or grossly reckless are given in Annex 3), including:

90.1. the means used by third parties to illegally lure personalised security features of payment instruments belonging to PSUs;

90.2. the novelty and complexity of the fraudulent act/instance affecting the user's ability to detect the fraud;

90.3. whether the PSU has taken adequate steps (or, on the contrary, has been found to have refrained from taking certain steps) to ensure that the confidentiality of the personalised security features of the payment instruments issued to them by the PSP, which enable them to initiate and authorise payments, is adequately protected;

90.4. in case the PSU has used its own authentication tool, whether and what the PSU has seen in its messages requesting PIN codes to confirm the disputed payment (i.e. whether the information is clearly displayed; when technologically enabled

by the capabilities of the authentication tool, to whom and for what purpose the password(s) for the authentication tool has been requested);

90.5. whether the personalised security features of the payment instrument have been misappropriated by third parties (fraudsters) during the normal use of the payment instrument by the PSU (e.g. whether the authenticator PIN codes have been entered for their intended purpose, i.e. using the relevant PIN code in the way it is normally used);

90.6. whether the PSU has been made aware by the PSP of the risks and ways of committing cyber fraud, as well as the meaning and legal consequences of the secure use of identification means and payment instruments issued by the PSP, the meaning and legal implications of entering and disclosing their personalised security features, the specificities (features and ways of protection) of the particular fraud case, etc.

90.7. other circumstances which, in the opinion of the PSP, contribute to the proper assessment of the PSU's conduct in a particular case.

91. The list of circumstances for assessing the behaviour of a PSU in paragraph 90 of the Guidelines is not exhaustive. The PSP should assess all the circumstances (in their totality and context) of the individual case which would justify the PSP's judgement that the PSU's conduct was prudent, reckless or grossly negligent in the specific case of the PSU's use of the payment instrument issued to them (in the performance of the duties imposed on them in relation to that payment instrument).

92. The PSU shall cooperate with the PSP and disclose to the PSP all the circumstances known to the PSU, as well as provide the PSP with the requested data, in order to enable the PSP to investigate the circumstances of the execution of the disputed payment transaction in detail and within the time limits established by law and to make a correct decision on the recognition of the disputed payment transaction as duly authorised and on the refund of the amount of this payment transaction or for the reimbursement of the amount of this payment transaction to the PSU. In case the PSU does not cooperate with the PSP (i.e. failure to disclose all the circumstances of the execution of the disputed payment transaction known to the PSU, failure to provide the available data (requested by the PSP), provision of false information and/or provision of false data), the decision of the PSP on the recognition of the duly authorised payment transaction and the refund of the

amount of this payment transaction to the PSU shall be taken by the PSP on the basis of the information and data known/available to the PSP.

93. The decision of the PSP to refuse to compensate the PSU for losses resulting from a disputed payment transaction in the case of fraud – whether the PSP determines that such a payment transaction has been authorised or whether it refuses to compensate the PSP for losses resulting from a payment transaction that has not been authorised by the PSP after assessing the PSU's behaviour as deliberate, fraudulent, dishonest, or grossly negligent – shall be evidence-based and well-reasoned, and be taken after having examined the totality of all the circumstances of the case in question.

94. The PSP refusing to reimburse the amount of the disputed payment transaction to the PSU shall inform the PSU in writing of the reasons for such a decision and provide the data (evidence) supporting the PSP's decision. The decision shall, inter alia, specify the procedure for challenging it, i.e. for complaints and/or disputes.

95. The additional possibilities for the PSU, as the holder of the payment card, to chargeback the funds from payment transactions made with a payment card are set out in the procedure established by the international payment card organisation, and do not remove the obligation of the PSP to reimburse the amount of the unauthorised payment transaction to the PSU in accordance with the procedure and within the time limits set out in the legislation, nor do they remove the obligation of the PSP to conduct a thorough investigation of the circumstances of the payment transaction disputed by the PSP and to adopt a reasoned and evidence-based decision in the event that it decides to refuse to reimburse to the PSU the amounts of the disputed payment transaction in accordance with the procedures and within the timeframes provided by the present Guidelines and legislation.

96. PSPs may also establish more favourable rules for the compensation of losses to PSUs resulting from disputed payment transactions carried out as a result of fraud and/or fraudsters. For example, by providing that it will compensate PSUs in certain cases for losses caused by authorised payment transactions or unauthorised payment transactions caused by the PSU's gross negligence.

CHAPTER VIII
FINAL PROVISIONS

97. It is recommended that PSPs make publicly available information related to fraud and fraud prevention that would allow PSUs to take into account the PSP's preventive efforts and the consequences of encountering fraud, including but not limited to the following information:

97.1. what the PSP's attitude is towards the importance of fraud prevention;

97.1. what educational measures the particular PSP uses;

97.2. what kind of fraud prevention and fraud response initiatives the PSP is involved in;

97.3. the ways in which fraud can be reported;

97.4. when and how a particular PSP contacts and identifies its PSUs (identification, as well as the ways in which a particular PSP identifies itself to PSUs).

Annex 1
SELF-ASSESSMENT OF THE EFFECTIVENESS OF THE FRAUD PREVENTION PROCESS

Internal governance

The managers of the PSP have a clear responsibility for the management of fraud risk, which should be treated in the same way as other risks faced by the PSP. There should be evidence of the active involvement of the managers of PSPs in addressing fraud risks. The managers of PSPs should have sufficient relevant information to understand the risks posed to the operations of PSPs by fraud.

Assessment questions:

- When was the last time that the managers of PSPs considered fraud risk issues? What actions followed these discussions?
- How do the managers of PSPs receive up-to-date information on the management of fraud risks and the effectiveness of prevention measures in place? (This may include receiving reports on performance in this area, as well as ad hoc briefings on individual cases or emerging threats.)
- Is there reasonable evidence to suggest that managers of PSPs have adequately assessed and addressed issues related to improving the effectiveness of fraud risk management? (Positive developments in the targets set by the PSPs.)

- What information do the managers of PSPs receive on fraud trends? Are fraud losses recorded clearly and separately from other losses?
- Do the managers of PSPs have a clear picture of which products, services and distribution channels are most vulnerable?
- How do the managers of PSPs respond when reported fraud increases?
- Do the investments of PSPs in anti-fraud systems reflect fraud trends?

Organisational structure

The organisational structures of PSPs for managing fraud risk and assessing the effectiveness of the prevention measures in place may vary. Some PSPs may have a separate unit or designate a dedicated staff member (FPO) to coordinate fraud risk management efforts, who may report to the head of risk, compliance officer or any other manager of the PSP as identified in the internal documents. Other PSPs may allocate responsibilities more broadly, with specific responsibilities, reporting lines and other organisational issues of fraud risk management being set out in internal procedures. There is no single correct answer here, but the organisational structure of PSPs should promote coordination and information sharing throughout the payment service provision process.

Assessment questions:

- Who bears ultimate responsibility for fraud prevention?
- Do PSP staff have the appropriate experience and competences, along with clear reporting lines?
- Does the organisational structure promote a coordinated approach and accountability?
- Do the managers of PSPs allocate sufficient resources to ensure that the fraud prevention function is carried out effectively? What are the annual budgets for fraud risk management and are they proportionate to the risks faced?
- Do the staff members responsible for fraud risk management have other functions? (The responsible staff members may be assigned other functions at the same time, but the potential for conflicts of interest should be assessed on an ongoing basis.)

Fraud risk management

PSPs identify and assess the fraud risks arising from, for example, the products and services they offer, the jurisdictions in which they operate, the types of customers they attract, the complexity and volume of transactions, and the distribution channels used to serve PSUs. PSPs can then direct their resources to the areas of highest risk.

Assessments carried out using a risk-based approach should:

1. Be comprehensive – it is usually not sufficient to consider only one factor.
2. Draw on a wide range of relevant information – it is usually not sufficient to consider only one source.
3. Be proportionate to the nature, scale and complexity of the PSP's activities.
4. Provide a holistic view of the risks associated with an individual relationship, considering all relevant risk factors for a particular PSU. (The assessment of risks associated with individual relationships can provide information for, but is not substitute for, business-wide risk assessments.)
5. Enable an appropriate level of due diligence to manage identified fraud risks.
6. Be regularly reviewed to remain relevant.

Assessment questions:

- What are the main areas of fraud risk?
- How does the PSP seek to understand the fraud risks it faces?
- When was the fraud risk assessment last updated?
- How are new typologies of fraud identified?
- Is there evidence that fraud risks are assessed and recorded systematically?
- Who initiates the fraud risk assessment and how? Is the process properly organised and documented?
- How quickly are fraud risk management policies and procedures updated in response to new fraud cases that are identified?

Fraud risk management policy and procedures

The fraud risk management policies and procedures of PSPs are commensurate with the scope and risk level of the payment services provided. They should be easily accessible and understandable to all staff members involved in fraud risk management.

Assessment questions:

- How often are the PSP's fraud risk management policies and procedures reviewed?
- How does the fraud risk management policy contribute to mitigating identified fraud risks? (Positive developments in the targets set by the PSPs.)
- What measures does the PSP take to ensure that fraud risk management policies and procedures reflect newly identified fraud typologies or external events? How quickly are necessary changes made?
- What steps does the PSP take to ensure that its staff understand the fraud risk management policies and procedures?
- How does the PSP ensure that fraud risk management policies and procedures are disseminated and applied to all staff members in the provision of payment services?

Staff awareness and professional development

In order to carry out their functions effectively, staff members must have sufficient knowledge and skills in fraud prevention. PSPs should review the competence of their staff and take appropriate action to ensure that they remain competent to carry out their duties. Further training should be consistent with the functions performed by the staff.

Assessment questions:

- How does the PSP ensure that its staff members are aware of the risks of fraud and their responsibilities in relation to fraud prevention?
- Are staff members able to receive training on fraud risks?
- Is the training tailored to the specific functions of the staff?
- Are the training materials relevant and up-to-date? When were they last reviewed?

- How is the effectiveness of training on fraud prevention assessed? (Positive developments in the targets set by the PSPs.)

Oversight

All PSPs want to protect themselves and their PSUs from fraud. This is supported by the oversight and tailored controls of the management tools in place, the risk assessment process and fraud data. PSPs should consider the implications of the scale of the fraud risk they face for their reputation, their customers and the markets in which they operate. The managers of PSPs should ensure that fraud risk management policies and procedures are appropriate and followed, for example, through robust internal audit and compliance processes that regularly review existing preventive measures.

Assessment questions:

- How does the PSU ensure that comprehensive reviews of the governance tools in place, the risk assessment process and fraud data are carried out?
- What are the findings of recent external/internal audits and compliance reviews on topics related to fraud prevention?
- How has the company implemented the recommendations for improvement resulting from the reviews?

Data security

PSPs must be alert to the risk of fraud associated with holding PSUs' data and have written data security policies and procedures which are proportionate, accurate, up to date and relevant to the day-to-day provision of payment services.

Assessment questions:

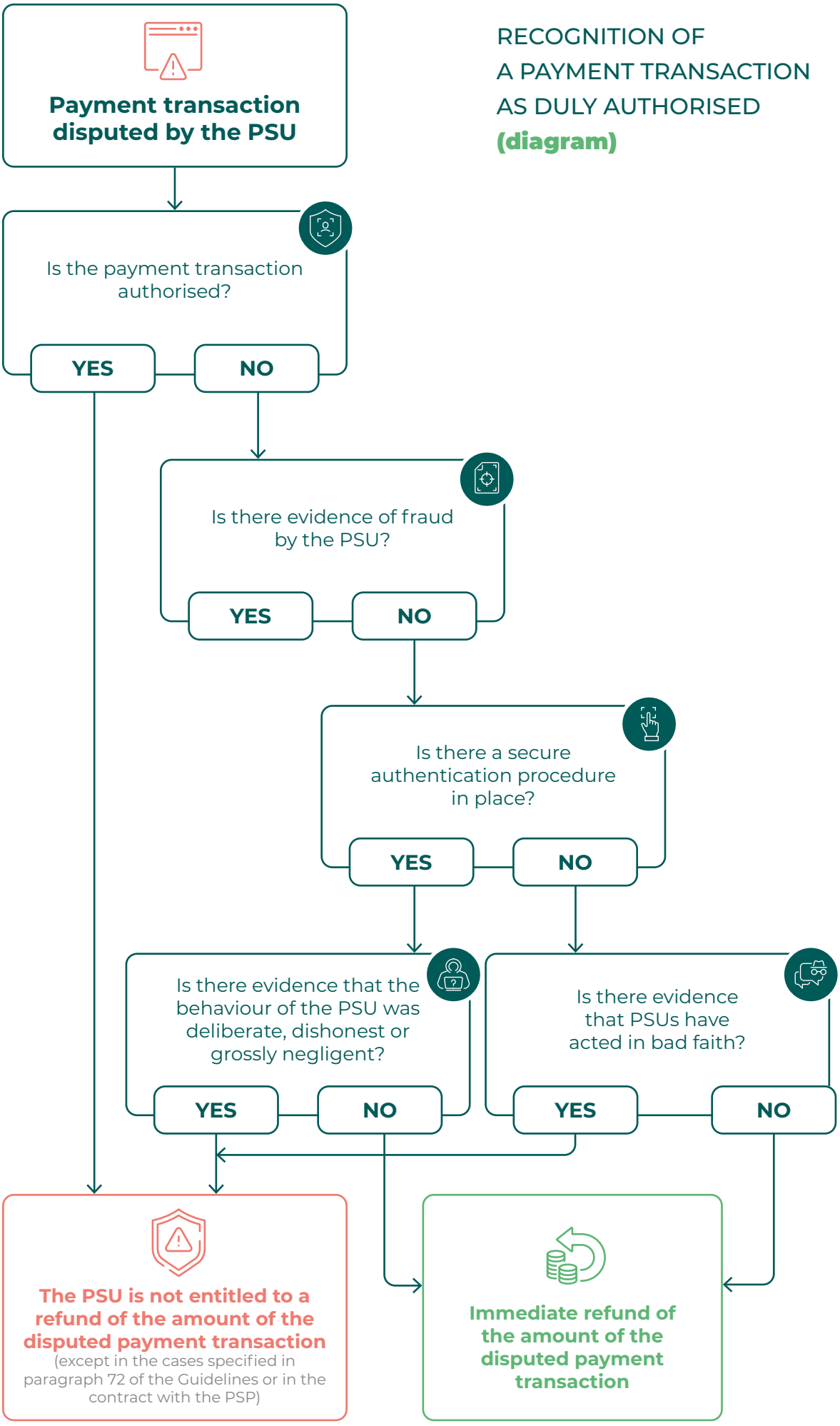
- How is responsibility for the security of PSU data allocated?
- Has the PSP ever lost the PSU data? If so, what remedial action has been taken? Have PSUs been informed? Has the PSP reviewed its systems?
- How is it ensured, if applicable, that outsourcing providers handle the PSU data properly, and how is this monitored?
- Is compliance with the data security standards set out in the outsourcing agreements monitored in conjunction with the suppliers?

Annex 2

RECOGNITION OF A PAYMENT TRANSACTION AS DULY AUTHORISED

diagram

RECOGNITION OF A PAYMENT TRANSACTION AS DULY AUTHORISED **(diagram)**

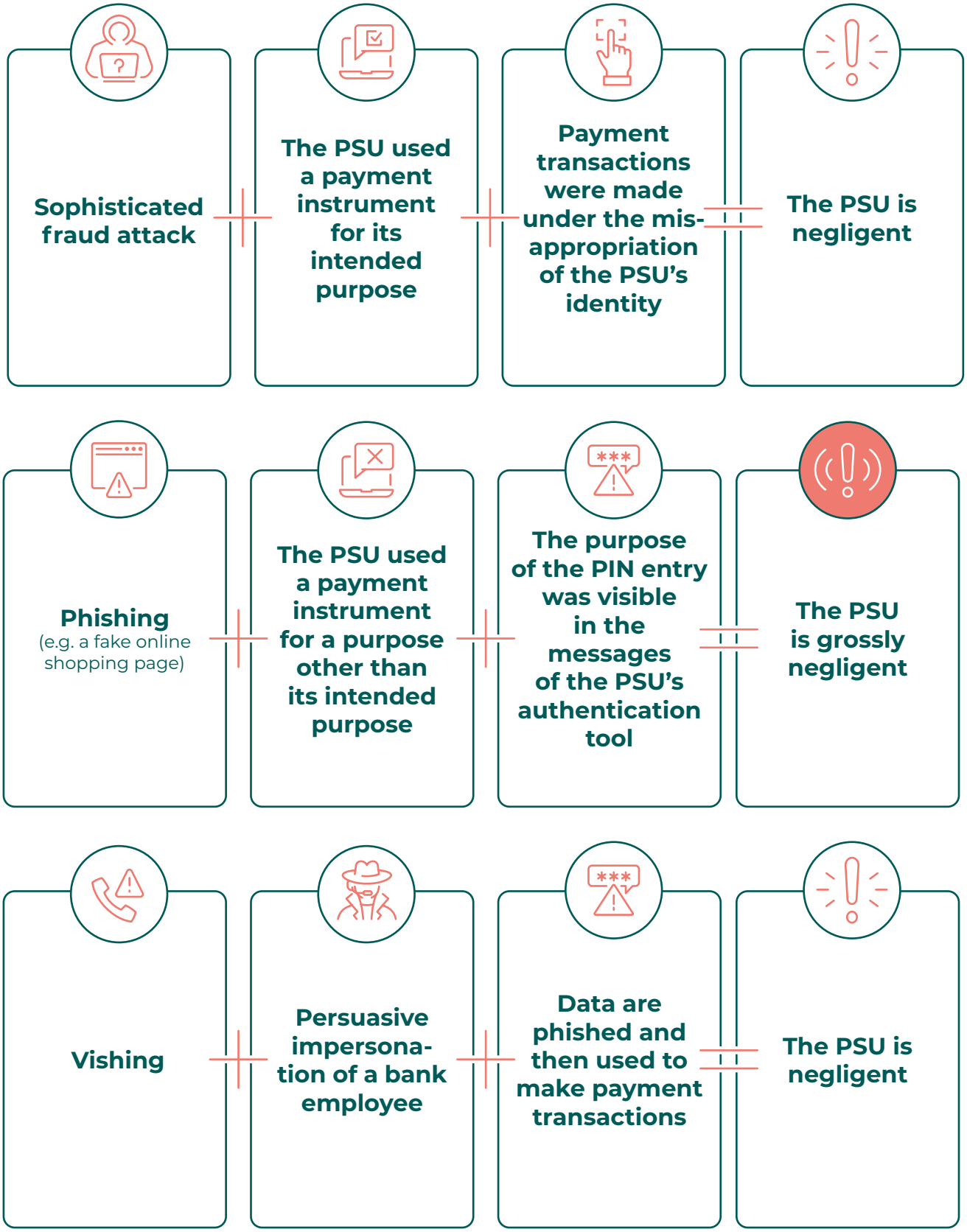


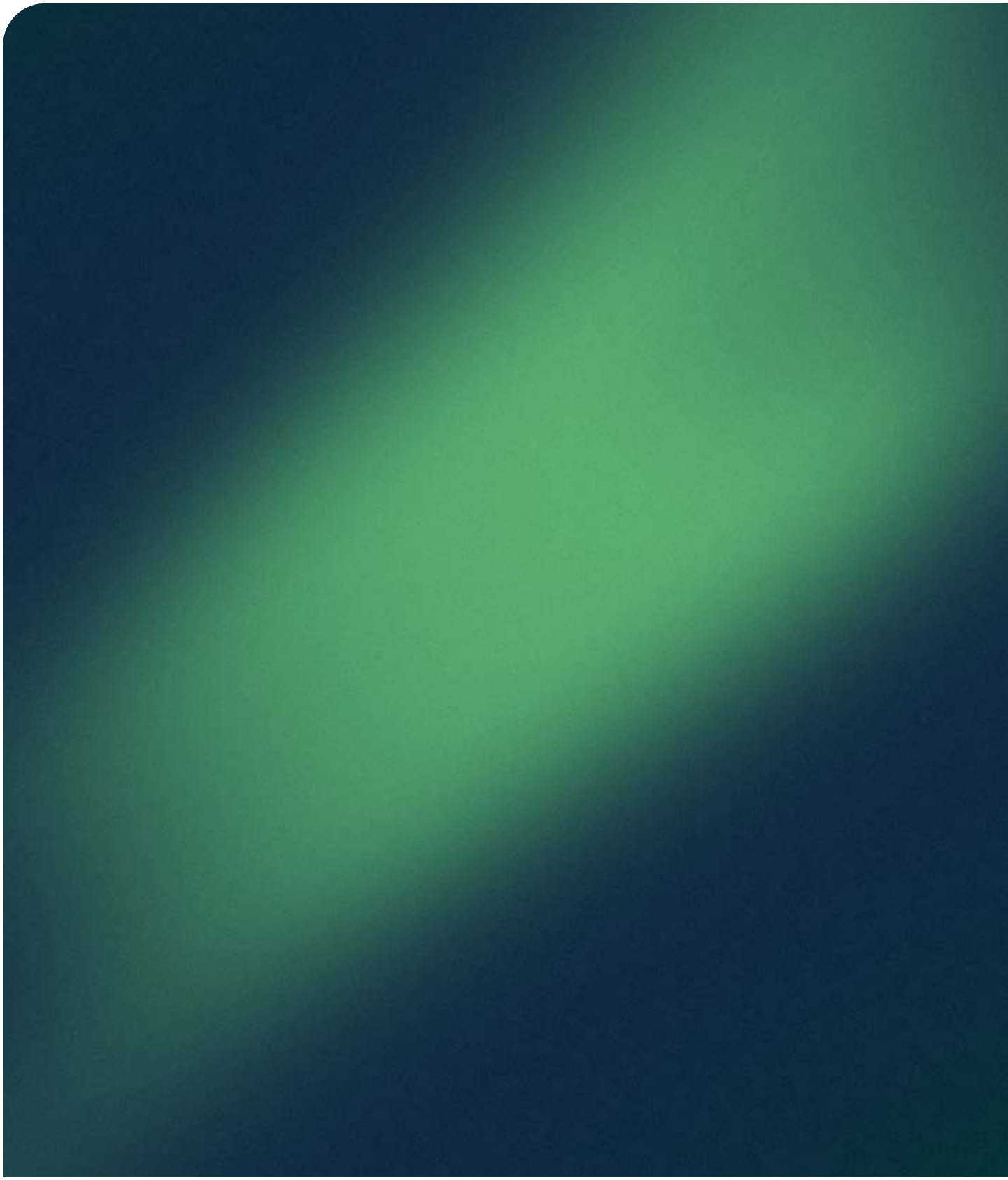
Annex 3
ASSESSMENT OF THE PSU'S BEHAVIOUR AS NEGLIGENT OR GROSSLY NEGLIGENT[7]

diagram

7 These are hypothetical examples which should not be considered to represent prior opinions of the Bank of Lithuania in any particular case. A decision on whether a particular PSU's behaviour is negligent, grossly negligent, intentional or fraudulent must be made only after a full analysis of all the relevant circumstances of the individual case.

ASSESSMENT OF THE PSU'S BEHAVIOUR AS NEGLIGENT OR GROSSLY NEGLIGENT **(diagram)**





LIETUVOS BANKAS

EUROSISTEMA