Methodological Guideline
of Financial Market Supervision Units of Národná banka Slovenska
No 4/2019 of 13 May 2019
regarding the prevention by payment institutions, electronic money institutions, payment service agents, branches of foreign payment institutions and branches of foreign electronic money institutions of money laundering and terrorist financing

The Financial Market Supervision Units of Národná banka Slovenska, on the basis of Article 1(3)(a)(3) of Act No 747/2004 on financial market supervision, as amended, in collaboration with the Ministry of Interior of the Slovak Republic, and the Financial Intelligence Unit of the National Crime Agency of the Police Force Presidium (hereinafter referred to as 'the FIU') has issued this Methodological Guideline:

Definitions

'Payment institution' means a legal person which may provide payment services under a granted authorisation.

'Electronic money institution' means a legal person, established in Slovakia, which under granted authorisations may issue and manage electronic money and conduct payment operations related to electronic money issuance (without limitation or in limited scope in accordance with Act No 492/2009 on payment services (and amending certain laws), as amended).

'Branch' means an organisational unit of payment institutions or electronic money institutions located in or outside Slovakia.

'Foreign payment institution' means a person established outside Slovakia which directly offers payment services on the basis of an authorisation granted in the country where it is established.

'Foreign electronic money institution' means a legal person, established outside Slovakia which directly issues electronic money on the basis of an authorisation granted in the country where it is established.

'Branch of a foreign payment institution or foreign electronic money institution' means an organisational unit of foreign payment institutions or foreign electronic money institutions located in Slovakia which directly offer payment services or issue electronic money; all branches of foreign payment institutions or foreign electronic money institutions established in the Slovak Republic by foreign payment institutions or foreign electronic money institutions established in another Member State are deemed to constitute a single branch.

'Payment service' means:
(a) placement of cash on a payment account and all the operations required for operating a payment account;
(b) cash withdrawals from a payment account and all the operations required for operating a payment account;

(c) execution of payment transactions, including transfers of funds from or to a payment account with the user's payment service provider (by credit transfer, through a payment card or another payment instrument, or by direct debit);
(d) execution of payment transactions where the funds are covered by a credit for a payment service user (in the form of an authorised overdraft on the payment account, or in the form of a credit facility through a payment card or another payment instrument);
(e) issuing of payment instruments and/or acquiring of payment transactions;
(f) money remittance;
(g) payment initiation services;
(h) account information services.

'Member State' means a Member State of the European Union or other country of the European Economic Area.

'Host Member State' means a Member State where the following is located:
(a) registered office of the payment service provider, or
(b) headquarters of the payment service provider, where the payment service provider has no registered office under his home-country law.

'Host Member State' means other Member State than the home Member State where the payment service provider has his payment service agent or branch or provides payment services.

Article 1
Purpose

(1) The purpose of this Methodological Guideline is to provide payment institutions, electronic money institutions, payment service agents, branches of foreign payment institutions and branches of foreign electronic money institutions (hereinafter referred to as 'financial institutions' or 'financial institution branches') or individually as a 'financial institution' or 'financial institution branch' a more detailed explanation for fulfilling their duties arising under legal regulations focused on the prevention of money laundering and terrorist financing in the financial system, which are based not only on binding Slovak legislation, but also international standards and, not least, on knowledge, experience and practice gained in the performance of supervision and control by Národná banka Slovenska (hereinafter referred to as 'NBS') and the Financial Intelligence Unit of the National Crime Agency of the Police Force Presidium (hereinafter referred to as 'the FIU').

(2) Financial institutions are required to comply with duties laid down by Act No 297/2008 on the prevention of money laundering and terrorist financing (and amending certain laws), as amended (hereinafter 'Act No 297/2008'), whilst proceeding also in accordance with other legal regulations, in particular Act No 492/2009 on payment services (and amending certain laws), as amended (hereinafter 'Act No 492/2009').

(3) In preparing this Methodological Guideline the authors based their work on the fact that the rules laid down by the legal regulations represent minimum requirements; the authors, through this Methodological Guideline, cannot give instruction for solving all cases that arise in practice. The rules do, though, give financial institutions the freedom to use other sources of information and to set their own rules, if necessary more stringent than those required by Slovak legislation. In accordance with the objective pursued by the above-mentioned acts and by this Methodological Guideline, financial institutions may also use more sophisticated methods,

particularly those already used and proven in their own practice or those of their parent companies from other Member States of the European Union (hereinafter referred to as the 'EU'). In so doing they can better contribute to the implementation of the global anti-money laundering and counter terrorist financing policy in the framework of the financial group of which they are part.

(4) The provisions of this Methodological Guideline apply mutatis mutandis to electronic money institutions, branches of foreign electronic money institutions and payment service agents under Article 75 of Act No 492/2009 that provide payment services for payment institutions in another Member State.

Article 2
The policy of protecting a financial institution against money laundering and terrorist financing

(1) A financial institution must have its own policy in the field of the prevention and detection of money laundering and terrorist financing (hereinafter the referred to as 'AML/CFT policy'). The AML/CFT policy must be set so as to ensure effective performance of activities aimed at preventing and detecting money laundering and terrorist financing at the financial institution.

(2) In setting and applying the AML/CFT policy a suitable tool and valuable source of information are Slovak and international standards, opinions and guidelines by Slovak and foreign regulators, analyses by major Slovak and foreign institutions or consultancy firms, and not least also the experience and the approach of other companies within the group of which the financial institution is part.

(3) In preparing and applying the AML/CFT policy, a financial institution takes into account in particular

(a) its business objectives and business plan;
(b) the structure of customers including their number and risk profiles;
(c) the range of activities and product types, geographic risks, distribution channels through which the products and services provided are carried out and the associated potential threat of their misuse for the purposes of money laundering and terrorist financing.

(4) The AML/CFT policy forms a part of risk management at the financial institution, with particular relevance to operational risk management.

(5) The policy includes:

(a) an organisational structure ensuring effective and independent performance of activities in the area of the prevention of money laundering and terrorist financing (hereinafter referred to as the 'AML/CFT area').
(b) a programme of own activity pursuant to Article 20 of Act No 297/2008 (hereinafter referred to as the 'Programme');
(c) information intended for customers and the general public, containing the financial institution’s approach and objectives in relation to AML, including a notice drawing attention to its duties of prevention and control that may have a direct impact on customers.

(6) Pursuant to Article 69(1) of Act No 492/2009 a financial institution's articles of association define in particular the financial institution's organisational structure and the division of powers and responsibilities of persons and units, including the AML/CFT area. In the framework of the organisational structure, the financial institution designates a member of the statutory body or a managerial employee as responsible for the area of AML (hereinafter as the 'Responsible Person'). The AML/CFT policy, in written form, is adopted by the statutory body, which is also responsible for implementing it.

(7) In the organisational structure pursuant to sub-paragraph 5(a), a foreign financial institution's branch designates a managerial employee as responsible for the AML area, or designates that the head of the branch is responsible for the AML area (hereinafter the 'branch's Responsible Person').

(8) The foreign branch's AML/CFT policy, in written form, is adopted by the branch's Responsible Person, who is also responsible for implementing it.

(9) A financial institution publishes the information and facts under paragraph 5(c) on its website.

Article 3
Employees responsible for implementing AML/CFT tasks, good repute of employees

(1) The statutory body of the financial institution is responsible for the financial institution's overall ML/TF prevention and for implementing the AML/CFT policy.

(2) A branch's Responsible Person is responsible for ML/TF prevention at the financial institution's branch and for implementing the AML/CFT policy.

(3) Responsibility for the practical implementation of activities in the AML area, primarily the performance of day-to-day activities ensuring the implementation of the AML/CFT policy, the reporting of unusual transactions and for ongoing contact of the financial institution with the Financial Intelligence Unit lies with the Nominated Officer.

(4) It is not appropriate to outsource the activities of the Nominated Officer.

(5) A financial institution ensures full substitutability of the Nominated Officer by means of a deputy.

(6) In filling the post of the Nominated Officer and deputy Nominated Officer, the financial institution requires demonstration of good repute, appropriate education and corresponding professional experience.

(7) The Nominated Officer and deputy Nominated Officer of a financial institution are appointed and dismissed by the statutory body, following prior consultation with the supervisory board. The financial institution's Nominated Officer reports directly to the financial institution's statutory body.

(8) The Nominated Officer of a financial institution's branch is appointed and dismissed by the Responsible Person or head of the branch. The Nominated Officer of a financial institution's branch reports to the Responsible Person of the branch or head of the branch.

Where a financial institution has several places in the Slovak Republic at which it performs its activities, it may nominate an employee at these places, who need not be a member of the unit responsible for performing activities necessary for ensuring tasks of the preventive system (hereinafter the 'Prevention Unit'), and entrust that employee with the performance of selected activities pertaining to the Nominated Officer or Prevention Unit (hereinafter the 'Authorised Employee'). The Authorised Employee is in continuous working contact with the Nominated Officer. If a financial institution also establishes a Prevention Unit, the Nominated Officer is the manager of that unit.

(9) An important element of a financial institution's AML/CFT policy is to ensure that the Nominated Officer, his deputy and the Prevention Unit have a sufficiently independent status in the structure of statutory bodies, managerial staff and organisational units. The Nominated Officer's classification in the financial institution's organisational structure contains the following elements guaranteeing an appropriately defined standing of the Nominated Officer, his deputy:

(a) arrangement of powers and duties of the Nominated Officer and his deputy in their job descriptions, with emphasis on the primary area of their operation, which is to ensure the financial institution's prevention in the AML area;
(b) separation from units responsible for customer products and services or payment transactions execution;
(c) unrestricted access of the Nominated Officer and his deputy to all documents, databases and information at the financial institution;
(d) autonomous and independent decision-making of the Nominated Officer and his deputy in assessing the unusualness of customers' transactions reported by the respective staff in the framework of the internal reporting system;
(e) autonomous and independent decision-making on the sending of unusual transaction reports to the FIU;
(f) control function of the Nominated Officer, his deputy, or the Prevention Unit in relation to units and staff responsible for customer products and services or payment transactions execution;
(g) separation of the Nominated Officer, his deputy, or the Prevention Unit from staff responsible for internal control in the organisational structure, whilst preserving follow-up inspection of their activity conducted by the staff responsible for performing internal control;
(h) in the case of extraordinarily serious circumstances or situations, immediate information to the statutory body, or the Responsible Person of the branch.

(10) The job description of the Nominated Officer includes in particular:

(a) ongoing preparation and updating of the Programme and any other necessary regulations and procedures for the AML area;
(b) the performance of management and control tasks in the AML area;
(c) communication and cooperation with the FIU; timely reporting of unusual transactions;
(d) communication and cooperation with NBS;
(e) organisation and setting of rules for the provision of training of the financial institution's staff, including new staff;
(f) analytical and advisory activity in relation to the assessment and reporting of unusual transactions by the respective staff in connection with the customer products and services or payment transactions execution.

(11) The Nominated Officer and his deputy are required to perform their duties with due professional diligence. The Nominated Officer of a financial institution submits a report on his

activity or on the activity of the Prevention Unit, if established, to the financial institution's statutory body at least once a year.

(12) The Nominated Officer of a financial institution's branch submits a report on the activities in the area of AML to the Responsible Person of the branch and to the head of the financial institution's branch at least once a year.

(13) The activity report contains in particular the following information:
(a) statistics and a brief description of unusual transactions reported by the financial institution's staff;
(b) statistics and a brief description of unusual transactions reported to the FIU;
(c) statistics and a brief description of unusual transactions that were not reported to the FIU, with the reasoning of non-reporting;
(d) overview of identified deficiencies and draft measures and deadlines for their rectification;
(e) information from inspections carried out;
(f) information or overview of relevant staff trainings conducted;
(g) statistics for identified deficiencies and cases of non-compliance with the staff's obligations.

(14) Before a person enters employment at the financial institution in a post or function where they will, in direct contact with customers, ensure the execution of payment transactions, the financial institution verifies the potential employee's criminal record check certificate, to establish that they have not been convicted of any property, economic or other serious crime.

(15) In addition to the criminal record check certificate under paragraph 14, a financial institution may require from the potential employee:
(a) information also beyond the framework of the criminal record check certificate (in such case however, it should be taken into account that if the conviction of a person has been expunged, this person is to be viewed as having a clean criminal record).
(b) a reference (or assessment) of his prior work integrity, issued by his previous employer, or
(c) other information.

(16) A financial institution should require from the potential employee several documents or more information relating to his good repute based on which a more objective assessment can be made of his good repute.

Article 4
Financial institution's Programme of own activity

(1) In accordance with Article 20 of Act No 297/2008, a financial institution shall prepare a programme that is approved by the financial institution's statutory body or head of the financial institution's branch. The Programme is based on generally binding legislation, in particular Act No 297/2008, Act No 492/2009 and other relevant laws and the FIU's methodological guidelines published and regularly updated on the FIU's website (http://www.minv.sk/?Metodicke-usmernenia-a-stanoviska-FSJ) as well as on the FATF Recommendations and the relevant EU legislation for the AML/CFT area.

(2) The Programme takes into account the financial institution's own specific characteristics, in particular

(a) its size and financial market share, organisational arrangement in terms of size, number of employees, management methods, the type and range of permitted activities, number of customers, the most common types of unusual transactions;
(b) its articles of associations and prevention policy;
(c) authorisations, duties, responsibilities and tasks of the Nominated Officer, internal control unit and internal audit unit;
(d) information flows, information systems, control processes and mechanisms in this area;
(e) procedures and duties of the financial institution's staff in the customer products and services or payment transactions execution;
(f) assessment, evaluation and updating of AML risks including the results of the National Risk Assessment in accordance with Article 26a of Act No 297/2008.

(3) The Programme sets out in particular:
(a) an overview of known types of unusual transactions, broken down by activity and type of product and service or payment transaction executed;
(b) detailed signs of unusualness by which unusual transactions can be recognised;
(c) methods of performing customer due diligence;
(d) the specification of the nature and extent of the implementation of customer due diligence on the basis of risk evaluation results pursuant to Article 10(4) of Act No 297/2008;
(e) the evaluation and management of risks associated with ML/TF, in accordance with Article 20a of Act No 297/2008, including customer assessment procedures based on a risk-oriented approach and risk analyses, taking account of the results of initial and ongoing customer identification and verification of their identification, broken down by type of product and service and payment transaction and type of account, as well as the risk category of customers;
(f) the nomination of persons at the financial institution who assess whether an intended or ongoing transaction is unusual;
(g) the setting of time or period when the assessment of a product, service or transaction is to be performed;
(h) the setting of how and in what way the assessment under sub-paragraphs (f) and (g) is to be performed, including the tools used in the assessment and recording of the assessment results;
(i) the method and scope of feedback at the financial institution on internal notifications of unusual transactions;
(j) the duty to maintain confidentiality regarding an internal notification of an unusual transaction and its reporting to the FIU and regarding measures performed by the FIU in accordance with Article 18 of Act No 297/2008, primarily in relation to the customer concerned, as well as toward persons having a certain relationship to the customer, and toward third parties, other than exceptions stipulated by Act No 297/2008;
(k) arrangements for the AML prevention, the receipt of notifications on identified unusual transactions from organisational units, the evaluation of these notifications and the reporting of unusual transactions to the FIU and arrangements ensuring ongoing working contact with the FIU, or law-enforcement bodies;
(l) the specification of tasks, duties and responsibilities for the financial institution's comprehensive AML prevention, at the individual levels of management from the statutory body of the financial institution, or from the Responsible Person of the financial institution's branch down to the units of first contact with the customer, including the internal control and internal audit units focusing on AML/CFT;
(m) the specification of information flows and description of information systems focused on the collection, processing and reporting of information for AML/CFT, including regular

reports submitted to the statutory body and supervisory board of the financial institution and Responsible Person of the financial institution's branch, or head of the financial institution's branch.

(n) the obligation to identify customers in executing products, services and individual financial transactions and the duty to verify this identification;
(o) the obligation to record the identification made and the verification of customers' identification;
(p) the obligation to retain records on customer identification and on the verification of their identification and on the financial transactions conducted by customers, and this for the period set by Act No 297/2008;
(q) the method and periods for retaining information and documentation;
(r) the nomination of the Nominated Officer pursuant to Article 20(2)(h) of Act No 297/2008;
(s) the procedure of the respective staff and Nominated Officer in delaying an unusual transaction under Article 16 of Act No 297/2008;
(t) the specification of basic tasks of the respective staff at all levels of management, the detection of unusual transactions and the reporting of internal notifications of unusual transactions to the Nominated Officer and the manner of ensuring the protection of the respective staff in connection with the unusual transactions identified by them and reported to the Nominated Officer;
(u) the content and timetable of staff training, training staff for performing AML/CFT tasks in the performance of particular activities, types of products and services and payment transactions of customers;
(v) the measures and control mechanisms preventing the abuse of position or function by staff to knowingly engage in money laundering or terrorist financing in the exercise of their function;
(w) an internal control system focused on AML/CFT, consisting of control mechanisms, process controls of managerial staff, including controls by the Nominated Officer and internal audits;
(x) a particular system of education including a training plan and the method of informing staff in accordance with Article 5(4).

(4) The AML/CFT issue requires that the Programme be drawn up as an integral regulation accessible to all the financial institution's staff in electronic or other form (Article 20(3) of Act No 297/2008).

(5) The Programme shall be updated at least once a calendar year. It is necessary to update the Programme in the case of a change in the relevant legislation of general application, in the case of changes concerning the own performance of the financial institution's activities and types of products, services and transactions, before new or innovative technologies and software solutions for products (transactions) and services are introduced, as well as in the case of changes to the financial institution's organisational arrangement.

Article 5
Staff awareness and training

(1) All staff of a financial institution must be aware that both a customer's knowing facilitation and a customer's unwitting involvement through negligence in money laundering or terrorist financing represents an operational risk. The financial institution can ultimately suffer financial losses if it executes transactions with proceeds from any criminal activity, whilst its reputation may also suffer.

Not only financial institutions as legal persons are subject to penalties for a violation or failure to fulfil duties in this field, but members of the statutory body, supervisory board, head of a foreign branch, the Responsible Person of a branch, managerial staff performing control and the respective staff in direct contact with the customer and who execute the customer's instructions for products, services and payment transactions may also be held liable.

(2) Success in applying an ongoing AML/CFT process depends on effective staff training and their proper familiarisation with duties and powers. The statutory body or the branch's Responsible Person, jointly with the Nominated Officer, ensure that staff are aware of the financial institution's responsibility, as well as of the personal responsibility of staff and their protection in the case of identifying and reporting unusual transactions in this area.

(3) A financial institution publishes in an appropriate manner information for staff about who performs the function of the Nominated Officer and who is his deputy.

(4) A financial institution determines in the Programme the optimal regime and method for:

(a) informing its staff about the AML/CFT system, and related procedures, duties and powers in the AML area;
(b) relevant staff members' access to the Programme and other regulations;
(c) organising regular training and educational activities for staff; where regular training is performed via e-learning, it is recommended to appropriately supplement e-learning training by other training forms, so that the training system is effective.

(5) A financial institution, in informing and training staff, takes account of its conditions, in particular its size and organisational arrangement, activities and types of product, service and financial transaction executed for customers, so that all necessary information reaches all staff for whom the information is intended. It is important that the mechanism of providing information to staff from the side of the statutory body, the Responsible Person of the branch, the Nominated Officer and respective managerial staff of the financial institution, as well as the model for performing staff training is effective, flexible and fulfils the desired objective; therefore, it is essential that it be updated with regard to changing conditions.

(6) The staff of first contact with the customer must have all necessary information on the activities, types of product, service and financial transaction they execute for customers and they must learn as soon as possible the criteria for assessing or detecting (forms of) unusual transactions.
These staff must be able to assess the conduct of the financial institution's customers, as well as the content of financial operations performed by customers in terms of their degree of risk, unusualness or suspiciousness. Staff training should significantly contribute to staff acquiring the prerequisites for mastering procedures for applying the Know Your Customer principle (hereinafter referred to as the 'KYC') and for recognising the degree of risk from the customer's actions, also with regard to the customer's categorisation into one of the three groups for mandatory customer due diligence:
- basic,
- simplified, and
- enhanced.

(7) In the framework of training, the financial institution ensures that staff are familiarised with the consequences of negligent fulfilment of their work duties and of any

knowing or unwitting participation in money laundering or terrorist financing, as well as the consequences of a breach of the prohibition of providing a customer with information to which the duty to maintain confidentiality applies (Article 18 of Act No 297/2008); as well as with the manner of their protection in the case of detecting an unusual transaction.

(8) The financial institution must have a plan of staff training prepared, taking into account the employee's work classification (own categorisation according to job positions, taking account of the employee's exposure to opportunities for and attempts at misuse for the purposes of money laundering and terrorist financing) and the resulting responsibilities, duties and the level and frequency of training pertaining thereto. The training plan, or its basic principles, should form a part of the Programme and should determine the basic outline, periodicity and content of staff training.

(9) Each employee concerned must be demonstrably familiarised with the applicable Programme governing procedures in assessing customers and their payment transactions, and concurrently the financial institution is required to ensure that each employee has permanent access to this Programme (Article 20(3) of Act No 297/2008).

(10) Staff training includes in particular:
(a) familiarisation with the Programme;
(b) familiarisation with Act No 297/2008;
(c) familiarisation with EU law;
(d) acquiring knowledge and information from the activities of:
1. the Nominated Officer;
2. other financial institutions;
3. the FIU, NBS;
4. national or international financial institutions in the AML/CFT area;
(e) AML case studies;
(f) initial training of new staff;
(g) specialised training,
(h) communication to staff the results of the training completed in accordance with paragraph 14.

(11) Initial training that staff should complete before they process customers' instructions for the execution of financial transactions should give them the necessary knowledge for ascertaining and verifying a customer's identity upon the creation of a business relationship and in the product and services and payment transactions execution.

(12) In determining the frequency of training (education), a financial institution observes the provisions of Article 20(3) of Act No 297/2008 (once per calendar year and always before an employee is assigned to work in which he performs tasks under the Act). A financial institution should repeat and supplement training (education) with new knowledge, where necessary, also more frequently than once a year, so as to ensure that the staff are able to continuously perform their duties and exercise their powers.

(13) A financial institution should apply and regularly update the following forms of training (education):
(a) standard (lectures);
(b) electronic (e-learning, tests, self-study of laws, etc.);
(c) work rotation;
(d) coaching and mentoring;

(e) random verification of knowledge of staff at the place of their work;
(f) combined forms in accordance with sub-paragraphs (a) to (f);
(g) other forms.

(14) A financial institution should include provision of feedback on the training (education) completed for the staff concerned. A financial institution should limit the number of repetitions in verifying the training (education) completed to the maximum number of repetitions (it is ineffective to be able to repeatedly verify training for example, in the form of a test without limitations to the number of repeated tests).

(15) A financial institution ensures that records are drawn on staff training (education) conducted, containing the date, content and form of the training, and, where relevant, an evaluation of the test completed, as well as the employees' signatures or other electronic confirmation.

(16) In training, staff acquires the necessary knowledge and capability to identify situations outside the customer's expected behaviour, and specific manifestations of unusual transactions. A financial institution should have the training (education) designed to respond to the ML/TF risks at any time horizon.

Article 6
Information system at a financial institution

(1) A systematic approach to the financial institution's risk management and AML/CFT requires the creation of appropriate information flows for ensuring the smooth, timely and regular flow of information between individual levels of management at the financial institution. A systematic approach for ensuring information flows requires support in the form of application software, i.e. a specialised information system, or systems.

(2) In broad terms the system under paragraph 1 means a system of acquiring, evaluating, transferring and using information concerning this area. This includes flows of information in the processes of the financial institution's individual activities and types of products, services and transactions performed within AML/CFT prevention.

(3) For the purposes of effective AML/CFT prevention, it is essential to ensure regular updates of the information system, with emphasis on the timely introduction of new types of product, service and transaction and procedure to the system.

(4) In addition to the information systems and application software for ensuring information flows for the AML/CFT system, the financial institution may, for support, use in addition to the manual system also a specialised automated system for detection of unusual transactions and persons subject to sanctions in the financial institution's relevant information systems, which operates on the basis of set scenarios on databases of customers, products and services or payment transactions.

(5) The financial institution is required to ensure information flows for:
(a) the transmission of information to staff on AML/CFT principles, procedures, duties and powers and the related performance of day-to-day tasks;
(b) making the Programme and other relevant internal regulations available to employees;

(c) transmission of necessary information between the Responsible Person and Nominated Officer;
(d) transmission of information between staff and the Nominated Officer and vice versa, including the internal reporting of unusual transactions;
(e) record-keeping, i.e. the recording, processing and updating of information on customers and the recording and monitoring of customers' payment transactions; communicating to the statutory body or Responsible Person the results of control performed by the Nominated Officer and staff responsible for performing internal control, as well as informing staff of these results;
(f) transmission of information between the Nominated Officer and FIU, including the reporting of unusual transactions and provision of other necessary information and source documentation to the FIU, as well as the provision of feedback from the FIU to the financial institution;
(g) searching for unusual transactions in the financial institution's relevant information systems that contain information on customers and their payment transactions.

(6) In ensuring information flows in accordance with paragraph 5(e), a financial institution should take into account also payment transactions and their AML risks.

(7) The form, content and rules of information are set by the financial institution taking account of its size, focus, scope and the complexity of its activities and on the types of products and services offered, as well as on the characteristics of its customers and their transactions.

(8) A component of a financial institution's information system is an electronic information system (hereinafter referred to as an 'EIS') that complies with statutory requirements, with the aim of ensuring sufficient quality in the prevention of money laundering and terrorist financing. An EIS recording and processing data on customers and their financial operations shall take account of the requirements provided for in Article 7(1) of Act No 297/2008:
(a) in the case of a customer - natural person, the EIS shall contain ascertaining of the following information: a customer's full name, personal identification number or date of birth if personal identification number has not been assigned, permanent address or any other address, citizenship, type and number of identity document and account number;
(b) in the case of a customer - natural-person entrepreneur, the same applies as under sub-paragraph (a) and also ascertaining their place of business address, registration number, if assigned, as well as the designation of the official register or other official record in which this entrepreneur is registered, and the number of their entry in this register or record.
(c) in the case of a customer - legal person, the EIS shall contain ascertaining of the following information: business name, registered office address, registration number, designation of the official register or other official record in which this legal person is registered and the number of their entry in this register or record, and identification data of a natural person authorised to act on behalf of the legal person, as under point (a).

(9) In addition to information referred to in paragraph 9, the EIS also contains information or records on the nature of a customer's business relationship; while the nature of a customer's business relationship is given by the type of product, service and transaction pursuant to Article 9(h) or solely by a transaction pursuant to Article 9(g) of Act No 297/2008, and it is primarily predetermined by the actual transaction that the customer uses. The EIS and the manner of using it should make it possible to identify unusual transactions performed by customers, and, as relevant, monitor also their course or development, as well as the connections

and links between the transactions of a certain customer and, where possible, also the unusual transactions of different customers.

(10) A special part of information recorded and monitored by the EIS consists in information on:
(a) politically exposed persons in accordance with Article 6 of Act No 297/2008;
(b) the beneficial owner in accordance with Article 6a of Act No 297/2008;
(c) shell banks in accordance with Article 9(d) and Article 24(1) of Act No 297/2008, which the staff received in performing their work tasks.

(11) The EIS should enable the financial institution to immediately provide the FIU, upon request, information as to whether it has or has had a business relationship with a specified person in the past five years, as well as on the nature of that business relationship in accordance with Article 21(2) of Act No 297/2008.

(12) The EIS should also enable to provide in a timely manner and sufficient scope data to the FIU, NBS and law enforcement authorities in cases specified by law, and not least, the EIS should also satisfy requirements for the purposes of control for the financial institution's own needs and for statistical purposes.

Article 7
Customer identification and verification, customer risk profile, basic, simplified, and enhanced customer due diligence

(1) The basic obligations and procedures of a financial institution in these areas are laid down in particular in the provisions of Articles 7, 8 and 10 to 13 of Act No 297/2008, Articles 31, 80, 88, and 88a of Act No 492/2009. As part of these procedures, a financial institution also verifies whether a customer is included in the list of persons subject to sanctions.

(2) Pursuant to Article 88(3) of Act No 492/2009 a financial institution is entitled in any transaction to require from a customer or payment service user, or his representative, for the purposes of ascertaining, verifying and checking identification, for the purposes of entering into and executing transactions in the provision of products and payment services under this Act, for the purposes of accepting and handling complaints and for other purposes referred to in paragraph 5 of this Act, the following data defined in paragraph (3)(a) of Act No 492/2009:
- in the case of a natural person, including natural persons representing a legal person, full name, permanent address, temporary address, personal identification number, if assigned, date of birth, nationality, and the type and number of their identity document;
- in the case of a natural person - entrepreneur, also their place of business address, field of business, as well as the designation of the official register or other official record in which this entrepreneur is registered, and the number of their entry in this register or record.
- in the case of a legal person, its name, company registration number, if assigned, registered office address, field of business or other activity, place of business address or the address of its organisational units and of any other place where its activities are performed, as well as a list of the members of the legal entity's statutory body and information on them as specified in point one, the designation of the official register or other official record in which this legal entity is registered, and the number of its entry in this register or record;

and acquire this information in the way specified in paragraph 3(b) of Act No 492/2009 by photocopying, scanning, or other means of recording.

(3) A financial institution performs all elements of basic customer due diligence (natural person and legal person) under Article 10(1) of Act No 297/2008 always in situations referred to in paragraph 2 of that provision of the Act. In the case of one-off products and services outside of a business relationship, the financial institution identifies and verifies identification always if the product and service value is at least €1,000. A financial institution may, based on the risk assessment under Article 20a of Act No 297/2008, set a lower value of transaction where the risk of money laundering and terrorist financing is higher.

(4) A financial institution ascertains whether the customer is acting on their own behalf; for the purposes of this Methodological Guideline the 'execution of a transaction on the customer's own payment account' or with their 'own funds' should be understood as the customer acting on their own behalf. According to Article 10(7) of Act No 297/2008 it is necessary to ascertain this fact always in the situations referred to in Article 10(2) even where this concerns a product or service at least in the amount of €15,000 and a product or service in the amount of €10,000 in cash.

(5) A financial institution identifies and verifies the beneficial owner in accordance with Articles 6a, 7, 8 and Article 10 of Act No 297/2008.

(6) In Article 6a of the AML Act, a beneficial owner is defined as a natural person who exercises control over a legal person, natural-person entrepreneur or property association, or a natural person in favour of whom these persons perform their activities or execute transactions. A beneficial owner may be in particular:

(a) in the case of a legal person that is not a trust, nor an issuer of securities accepted for trading in the regulated market, which is subject to the requirement to disclose information under a separate regulation, an equivalent legal regulation of a Member State or an equivalent international norm, a natural person who:
    1. has a direct or indirect share or a sum of direct and indirect share of at least 25% of voting rights or share capital in the legal person, including bearer shares;
    2. has the right to appoint, otherwise establish, or dismiss the legal person's statutory body, management body, supervisory board or control body, or the members thereof;
    3. has the ability to exercise control over the legal person in a manner other than as provided under points 1 and 2;
    4. is entitled to receive a profit share of at least 25% from the legal person's business activity or other activity;
(b) in the case of a natural-person entrepreneur, a natural person entitled to receive a profit share of at least 25% from the natural-person entrepreneur's business activity or other activity;
(c) in the case of a trust, a natural person who:
    1. is the founder or settlor of a trust; or if the founder or settlor is a legal person, a natural person as referred to in sub-paragraph (a);
    2. has the right to appoint, otherwise establish, or dismiss the trust's statutory body, management body, supervisory board or control body, or the members thereof, or who is a member of the body entitled to appoint, otherwise establish, or dismiss these bodies or their members;
    3. is the trust's statutory body, management body, supervisory board, control body or a member of these bodies;
    4. is a recipient of at least 25% of the funds provided by the trust, where the future recipients of these funds have been determined; if the future recipients have not been determined,

the beneficial owner will be a circle of persons who benefit significantly from the trust's establishment or operation.

(7) A financial institution should carry out the identification of the beneficial owner pursuant to Article 6a of Act No 297/2008 always in the case of:
(a) a legal person as referred to in Article 6a(1)(a) of Act No 297/2008;
(b) a natural-person entrepreneur as referred to in Article 6a(1)(b) of Act No 297/2008;
(c) a trust as referred to in Article 6a(1)(c) of Act No 297/2008.

(8) Where no natural person complies with the criteria pursuant to Article 6a(1)(a) of Act No 297/2008, the beneficial owner is deemed to be a member of the person's top management which may be:
(a) the statutory body;
(b) a member of the statutory body;
(c) the authorised representative, and
(d) a senior employee reporting directly to the statutory body.

(9) In identifying the beneficial owner, a financial institution ascertains with the person's
(a) under paragraph 7(a) their business name, registered office address, registration number, designation of the official register or other official record in which this legal person is registered and the number of their entry in this register or record, and identification data of a natural person authorised to act on behalf of the legal person;
(b) under paragraph 7(b) their full name, personal identification number or date of birth if a personal identification number has not been assigned, permanent address or any other address, citizenship, and type and number of their identity document, their place of business address, registration number, if assigned, as well as the designation of the official register or other official record in which this entrepreneur is registered, and the number of their entry in this register or record;
(c) under paragraph 7(c) information under sub-paragraphs (a) or (b) depending on whether the beneficial owner is a natural person.

(10) A financial institution identifies the beneficial owner and takes appropriate measures for verification of their identity pursuant to Article 7(1)(a) and in accordance with Article 10(1)(b) of Act No 297/2008.

(11) Where the conditions under Article 8(3) and (4) of Act No 297/2008 are complied with, the verification of the beneficial owner identification may be completed during the contracting of a business relationship.

(12) The obliged person under Article 10(1)(b) of Act No 297/2008 is required to carry out the identification of the beneficial owner and adopt appropriate measures for verification of their identity, including measures to determine the ownership and management structure of a customer (for example acquire information on shareholders, partners, management bodies) which is a legal person or a trust; when identifying the beneficial owner, the obliged person shall not rely exclusively on data from the register of legal persons, entrepreneurs, and public sector entities. If there are doubts about the correctness or completeness of data on the beneficial owner obtained previously, a financial institution shall perform once again the basic customer due diligence under Article 10(2)(d) of Act No 297/2008. If a financial institution cannot identify the beneficial owner and take appropriate measures to verify his identity, including

measures to ascertain the ownership and management structure of a customer, it shall reject or terminate a business relationship or refuse to execute the customer's instructions for particular products, services and transactions.

(13) Under Article 10(1)(d) of Act No 297/2008, a financial institution shall ascertain if the beneficial owner is a politically exposed person or person included in the list of persons subject to sanctions.

(14) The beneficial owner is ascertained always in the case of legal persons, whilst the legal form cannot affect the verification of the beneficial owner.

(15) When identifying the beneficial owner risks, financial institutions should in particular consider information on the risk factors under Annex 1 (in particular part 2.1.1 of Annex 1).

(16) In the case of new customers, in addition to the basic customer due diligence a financial institution assigns the customers to a particular risk category based on which the customer's risk profile can be created.

(17) When categorising customers to a certain risk category, a financial institution takes account of information on the risk factors under Annex 1 (in particular part 2 of Annex 1).

(18) A financial institution continuously updates the customer's risk profile according to the risk category to which the customer is assigned. A financial institution includes the time limits for updating the customer's risk profiles to the Programme.

(19) Based on the categorising of customers according to their risk profile a financial institution then applies ongoing monitoring of the business relationship pursuant to Article 10(1)(g) of Act No 297/2008, which leads to recognition and reporting of unusual transactions.

(20) A financial institution applies simplified customer due diligence to the extent and under the conditions referred to in Article 11 of Act No 297/2008. A financial institution may apply simplified customer due diligence, taking into account a risk-based procedure, when information concerning them can be obtained from publicly available sources and if at the same time the information sufficiently justifies the use of simplified customer due diligence. When applying simplified customer due diligence, a financial institution takes into account also the procedure under Annex 1 (in particular part 3 chapter 3.1 of Annex 1).

(21) Applying simplified customer due diligence does not mean that the financial institution is exempt from the obligation to carry on ongoing monitoring of the business relationship pursuant to Article 10(1)(g) and other obligations pursuant to Articles 14, 17, 19 and 21 of Act No 297/2008.

(22) A financial institution applies enhanced customer due diligence to the extent and under the conditions referred to in Article 12(2) of Act No 297/2008 which leads to risk mitigation to acceptable level. When applying enhanced customer due diligence, a financial institution takes into account also the procedure under Annex 1 (in particular part 3 chapter 3.2 of Annex 1).

(23) A financial institution applies enhanced customer due diligence mainly in:

(a) products and services that pose a higher risk with regard to their nature;
(b) special categories of customers and entities.

(24) Identification of a customer - natural person, without the customer being physically present, through technical means and procedures under Act No 297/2008 are set out in detail in Opinion No 1/2018 of the Financial Market Supervision Unit of Národná banka Slovenska of 10 December 2018 published on the NBS website:
(http://www.nbs.sk/_img/Documents/_Legislativa/_Vestnik/Stanovisko1_2018.pdf).

(25) The conditions for the proper application of the KYC principle derive from the duties of the financial institution and customer, as set out in the provisions of Articles 10 to 12 of Act No 297/2008. The crucial provisions are those of Article 10(1), (4) and (5) and Article 11(3) of the AML Act. The procedure under the provisions of Article 10(1) and Article 11(3) of Act No 297/2008 enables a financial institution to satisfy itself as to the actual identity of each customer and identify the purpose and planned nature of business activities that a customer will probably conduct. This procedure is also the starting point for a financial institution in determining the customer's risk profile, subsequent determining the degree of customer due diligence pursuant to Article 10(4) of Act No 297/2008 and accepting a customer. A financial institution then, depending on the result, shall apply procedures in the framework of basic customer due diligence under Article 10 or simplified customer due diligence under Article 11 or enhanced customer due diligence under Article 12 of Act No 297/2008.

Article 8
Detection, reporting and delaying of unusual transactions

A financial institution shall always assess whether a prepared or executed transaction is unusual. Under Article 20(1) and (2)(d) of Act No 297/2008 a financial institution must regulate this part of the procedures in its Programme. Duties referred to in Article 14(1) and (2)(a) and (b) of Act No 297/2008 must be fulfilled demonstrably so that the financial institution can, in accordance with Article 30(3) No 297/2008, in the case of an inspection, provide information and written documents on the fulfilment of these duties. Records on the assessment of transactions shall be archived for 5 years based on Article 30(3) in conjunction with Article 33(5) of Act No 297/2008.

(2) Under Article 4 of Act No 297/2008 an unusual transaction is a legal act or other act that indicates that its execution may lead to money laundering or terrorist financing.
Article 4(2) of the Act provides a demonstrative presentation of unusual transactions. In each unusual transaction listed in this provision there are, however, several indicators of unusualness (e.g. an unusually high amount of funds with regard to the type of transaction, an unusually high amount of funds without clear economic or legal purpose, etc.) that the financial institution is required to assess. Only by such action can it competently assess whether a customer's intended or ongoing transaction is unusual or not. Act No 297/2008 in Article 4 does not stipulate any criteria, e.g. in the form of threshold amounts of funds that would lead to the automatic finding in the case of a certain type of financial transaction that it undoubtedly constitutes an unusual transaction. A crucial element for assessing customer transactions is the application of the KYC principle and skilled identification of signs of unusualness, as well as other signs or criteria that the financial institution is required to determine for itself, depending on the subject and scope of its activity and the type and extent of products, services and financial transactions performed for customers, in the framework of drawing up an overview of the types of unusual transaction (Article 20(2)(a) of Act No 297/2008).

(3) A financial institution is required, regardless of the applied type of customer due diligence, to assess whether an intended or ongoing transaction is unusual (Article 14(1) of Act No 297/2008) and to pay particular attention to all complicated, unusually large transactions and all transactions of an unusual nature that do not have a clear economic purpose or clear legal purpose and to make an appropriate record on them in accordance with Article 14(3) of Act No 297/2008 (i.e. 'internal report of a potential unusual transaction'); it is also necessary to archive these records in accordance with the period referred to in Article 19 of Act No 297/2008.

(4) A financial institution performs skilled assessment of intended and ongoing products, services and financial transactions under Article 14 of Act No 297/2008 at various time intervals and at various levels. The assessment process takes place:

(a) on the frontline, where the financial institution's staff are in contact with an existing or potential customer;
(b) in the framework of ongoing monitoring of an existing business relationship;
(c) in the framework of subsequent (retrospective) assessment of a customer's transactions.

(a) assessment of products and services at initial contact with the customer before and during products and services or financial transaction execution

The assessment of products and services or transactions used by a customer is performed by staff of the financial institution who, in fulfilling their duties, are in contact with the customer, particularly those staff who receive or process a customer's instructions for products and services or payment transactions execution.

The assessment of a product, service or payment transaction by an employee of the financial institution is, thus, performed largely at the place of executing the financial transaction and prior to its performance, or at an attempt to execute a financial transaction so that an unusual transaction can be delayed and promptly reported.

A crucial element for assessing customers' business transactions is the appropriate application of the KYC principle and its procedures and skilled identification of signs of unusualness. This procedure enables the employee to assess a customer's intended or ongoing products, services and transactions by comparing them against an overview of types of unusual transactions (Article 20(2)(a) of Act No 297/2008), as well as against forms referred to in Article 4(2) of Act No 297/2008 and to detect those that are unusual in relation to the customer and his otherwise usual products and services and financial transactions.

If an employee judges an intended or ongoing transaction to be unusual, he makes a written record on this transaction in accordance with Article 14(3) of Act No 297/2008 and promptly notifies this finding to the Nominated Officer (hereinafter simply 'notification of unusual transaction').

(b) Assessment of products and services and transactions in the framework of ongoing monitoring of a business relationship

Depending on whether it concerns:

1. an existing business relationship (Article 10(2)(a) of Act No 297/2008), or
2. an occasional transaction (Article 10(2)(b) and (c) of Act No 297/2008), the competent staff of the financial institution assesses the customer's products, services and financial transactions also in the framework of ongoing monitoring of the business relationship.

The assessment of intended or ongoing products, services and financial transactions in the framework of ongoing monitoring of the business relationship is specific in that the business

relationship has already started and still continues (Article 10(2)(a) of Act No 297/2008). The customer may also be known to the financial institution where the customer has already executed several occasional transactions (Article 10(2)(b) or (c) of Act No 297/2008). Therefore, this is not the first contact with the customer and the financial institution may take account of the customer's existing risk profile and history of transactions performed by the customer.

The procedure according to Article 10(1)(d) of Act No 297/2008, including verification of the completeness and validity of identification data and information under Article 10(8) of the Act and the customer's duty under Article 10(5) of the Act form the basis for ongoing monitoring of the business relationship. This type of monitoring requires the creation of customer risk profiles and their classification with regard to the possible risk of money laundering and terrorist financing under Article 10(4) of Act No 297/2008.

Ongoing monitoring of the business relationship requires the use of an appropriate EIS that enables the financial institution, in accordance with risk-based prevention, to create financial or other criteria or limits as indicators of unusualness in customers' financial transactions so as to allow their differentiation into certain levels of the monitoring process, corresponding to the degree of risk inherent in the transactions performed by customers. The criteria or limits defined by the institution for this purpose must be regularly verified so that it is possible to determine their adequacy in regard to the identified levels of risk. The financial institution is required also to regularly review the adequacy of the existing system and individual processes of protection and prevention. For assessing products and services, importance is given, in the framework of ongoing monitoring of the business relationship, to intended or ongoing customer's products and services that do not correspond to the customer's known or expected activity or that correspond to types of unusual transactions referred to in the Programme or in Article 4(2) of Act No 297/2008. Such products and services or transactions of a customer form the subject of assessment (Article 14(2) of the Act) and it is necessary to make a written record of them (Article 14(3) of the Act); these records must be archived in accordance with the period referred to in Article 19 of Act No 297/2008.

The Nominated Officer may, based on results from the assessment of the various circumstances of a product, service and financial transaction, and with regard to the overview of types of unusual transaction (Article 20(2)(a) and Article 4(2) of Act No 297/2008 reach the conclusion that in the given case it does not constitute an unusual transaction. Where it is impossible to assess the transactions solely based on the customer information already available to the financial institution, it may, according to circumstances, request other necessary information and documents from the customer, pursuant to Article 10(5) of Act No 297/2008.

In cases where the Nominated Officer is unable, even through this procedure, to identify the reason for the customer's products and services and financial transactions that do not correspond to the customer's risk profile or known or expected activities, it is sufficient that these transactions merely indicate the fact that their execution may constitute money laundering or terrorist financing, and the Nominated Officer is required to proceed according to Article 17 of Act No 297/2008, i.e. to report the unusual transaction to the FIU.

The assessment of products and services in the framework of ongoing monitoring of the business relationship is performed, depending on the product and service and financial transaction, by staff as well as the Nominated Officer.

(c) Assessment of products and services in the framework of subsequent or retrospective assessment of a customer's transactions

A means of subsequent monitoring of customers' products and services and financial transactions is, for example ex-post random selection of executed instructions for products and

services and financial transactions in the framework of an inspection from the side of a manager superior to the employee who executed the customer's transactions, as well as in the framework of an inspection performed by the Nominated Officer and internal control unit.

(5) The recommended procedure in the processing and handling of internal notifications of unusual transactions and unusual transaction reports is as follows:

(a) all internal records of unusual transactions sent by the relevant employees to the Nominated Officer shall be documented in accordance with the provisions of Article 14(3) of Act No 297/2008 and shall be made available for the purposes of control under Article 29 of the Act;

(b) the sending of internal notifications and reports to the Nominated Officer may not be subject to the prior consent of any person;

(c) the Nominated Officer shall register and archive notifications on internal notifications of unusual transactions, including the position, first name, last name, workplace or unit of the financial institution and all data on the given customer and transaction in accordance with Article 19 of Act No 297/2008;

(d) the Nominated Officer, as well as staff of the financial institution, including its managers (and members of the statutory body) involved in assessing products and services under Article 14 of Act No 297/2008 are required to maintain confidentiality on reported unusual transactions and on measures taken by the FIU (Article 18 of the Act), including the fulfilment of duties under the provisions of Article 17(5) and Article 21 of the Act; the financial institution may not, however, cite toward Národná banka Slovenska and a competent authority the duty to maintain confidentiality in connection with the performance of supervision and inspection under Article 29 of the Act (Article 18(5) of the Act). Provided that information given is used exclusively for the purposes of preventing money laundering or terrorist financing, the duty of confidentiality does not apply to the provision of information between credit or financial institutions under the conditions set out in Article 18(8)(a) and (c) of Act No 297/2008;

(e) The financial institution is required to draw up a procedure covering the period from the moment of detecting an unusual transaction through to prompt reporting of the unusual transaction, including the procedure and responsibility of staff who assess the product and service;

(f) The Nominated Officer, after receiving an internal notification of an unusual transaction, may confirm receipt of the unusual transaction notification to the employee who sent the notification. The confirmation should contain an instruction on the duty to maintain confidentiality under Article 18 of Act No 297/2008. Where the financial institution has an electronic system of gathering internal reports that enables the competent employee to monitor the status or receipt of a submitted internal report of an unusual transaction by the Nominated Officer, or by the Prevention Unit, no individual confirmation of receipt of such a notification is needed;

(g) The internal notification of an unusual transaction, or the conduct of a customer, the product and service and/or financial transaction that the notification concerns shall be the subject of an assessment by the Nominated Officer, who may, on the basis of results from further assessment of the various circumstances of the product, service or financial transaction, and with regard to the overview of types of unusual transaction (Article 20(2)(a) of the Act) and Article 4(2) of Act No 297/2008, decide whether it does or does not constitute an unusual transaction. This internal notification contains information on the economic or lawful purpose of the financial operations and, in the case that it is a usual transaction, also sufficient reasoning or statement of information and reasons regarding its usual nature. Otherwise the process of such assessment cannot be considered trustworthy and objective. Where it is impossible to decide about the transactions solely based on the customer information already

available to the financial institution, it may, according to circumstances, request other necessary information and documents from the customer, pursuant to Article 10(5) of Act No 297/2008. Where the Nominated Officer reaches the justified conclusion that in the case of an internally notified unusual transaction it does not actually constitute an unusual transaction, the Nominated Officer is required to document this decision in writing and to archive all related data, written documentation and electronic documentation in accordance with the period referred to in Article 19 of Act No 297/2008;

(h) In cases where the Nominated Officer cannot even through this procedure reach the conclusion that it is not an unusual transaction, it is sufficient that the reported product and service and/or financial transaction indicate that their execution may constitute money laundering or terrorist financing, and the Nominated Officer is required to proceed according to Article 17 of Act No 297/2008, i.e. to report the unusual transaction to the FIU.
According to Article 17(1) of Act No 297/2008 an unusual transaction or attempt at executing an unusual transaction must be reported to the FIU promptly, i.e. at the earliest opportunity. It is always necessary to take into consideration the particular circumstances of the situation in which the finding of the unusual transaction is made, whilst a financial institution is required to report an unusual transaction as soon as possible. A decision of the Nominated Officer to report an unusual transaction must not be subject to the prior consent or approval of any other person. A report of an unusual transaction contains information specified in Article 17(3) and may not contain information referred to in Article 17(4) of Act No 297/2008. The reference number of each report of an unusual transaction should take the form: serial number / year / character code of the financial institution. An unusual transaction may be reported in writing, electronically or by telephone (in this case it is necessary to report the unusual transaction also in person, in writing or by e-mail within 3 days). The specimen form for reporting an unusual transaction, issued by the FIU, is given on the website (http://www.minv.sk/?vzory). An unusual transaction report may be supplemented at the financial institution's own initiative within 30 days. After this period, it is necessary to additionally report information and documentation acquired as another unusual transaction (or, based on an agreement with the FIU by telephone, as a supplementing information to the previous unusual transaction). In this subsequent unusual transaction, the financial institution states the unusual transaction to which the additionally acquired information and documentation relate. In connection with the reporting of unusual transactions and sending of further supplementary information, as well as the overall communication and exchange of information with the FIU, it is recommended in the interest of compatibility and streamlining of the procedure in the reporting process, as well as in the interest of streamlining control processes, that financial institutions communicate with the FIU by electronic means via the electronic registry, while complying with the conditions for protection of transmitted information and for clear identification and verification. Only in this way it is possible to avoid security risks connected with the reporting of unusual transactions;

(i) Article 18(8)(a) of Act No 297/2008 allows financial institutions, under defined conditions, to exchange information where this is reasonable and related to the threat of money laundering or terrorist financing, and where it helps obliged entities to more effectively assess a customer's products and services and financial transactions, as well as to alert other obliged entities to identified risks. An exchange of information may not contain the full scope of the reported unusual transaction as a whole, but only specific information relating to the risk of money laundering or terrorist financing. Information provided may, pursuant to the Act, be used exclusively for the purposes of preventing money laundering or terrorist financing.

(6) Recommended procedure in delaying an unusual transaction:

(a) according to Article 16 of Act No 297/2008, a financial institution delays an unusual transaction, i.e. a particular product, service and/or financial transaction (Article 9(h) of the Act) that would otherwise be executed;

(b) unless there is from the side of the customer an act or expression of will to use a product, service or execute a financial transaction, the financial institution has no transaction to delay;

(c) a financial institution is required under Article 16(1) of Act No 297/2008 to delay an unusual transaction until the time of its reporting to the FIU, whilst account is always taken of the operating and technical possibilities, as well as the moment when the financial transaction was or should have been assessed as unusual; e.g. a customer's transaction assessed in the framework of ex-post or retrospective assessment of the customer's transactions can no longer be delayed;

(d) a financial institution is required under Article 16(2) of Act No 297/2008 to delay an unusual transaction in the following two cases:

1. a financial institution delays an unusual transaction at its own discretion if execution of the unusual transaction poses the risk that there may be frustrated or substantially impeded the seizure of proceeds from crime or seizure of funds intended for financing terrorism; in such a case the financial institution is required to immediately inform the FIU of the delaying of the unusual transaction;
2. a financial institution delays an unusual transaction if the FIU requires it in writing;

(e) a financial institution does not delay an unusual transaction if it is unable to do so for operating or technical reasons (it immediately notifies the FIU of this fact) or if delaying the unusual transaction could, according to a previous notice from the FIU, frustrate the processing of the unusual transaction;

(f) the period of delaying of a transaction by a financial institution pursuant to Article 16 of the Act is no more than 120 hours; therefore, if during this period the FIU notifies the financial institution that it has forwarded the case to the law enforcement authority, the financial institution is required to extend the period of delaying, though no more than by a further 72 hours. Therefore, the total duration of delaying of an unusual transaction is no more than 192 hours. If during the period of delaying of an operation the financial institution receives no instruction to seize funds from the side of a judge or prosecutor pursuant to Article 95 or 96 of Act No 301/2005 the Code of Criminal Procedure, as amended (hereinafter referred to as the 'Code of Criminal Procedure'), the financial institution executes the delayed transaction following the expiry of the set period. Prior to the expiry of the delaying period, the financial institution may execute the transaction only in the case that the FIU notifies it in writing that from the aspect of processing the unusual transaction, its further delaying is not necessary. Weekends and bank holidays are not counted in the delaying of an unusual transaction.

The period of delaying of an operation pursuant to Article 16 of Act No 297/2008 is deemed to begin at the moment when the customer expresses the intention (will) to execute a financial transaction. In the case that a financial institution presumes that the customer will express an intention to execute an unusual transaction in the future, it is required to take personnel, organisational and technical measures so that in the case that the customer does give such instruction, it is not executed and thereby any potential delaying of the unusual transaction is not frustrated. The period of delaying of a transaction pursuant to Article 16 of the Act may not be deemed to begin as of when the financial institution evaluated the executed financial transactions as unusual or learnt of the customer's executed transactions. Likewise, the reason for delaying a transaction may not be the fact that the customer requested from the financial

institution general information regarding a payment account (information on the account balance, etc.).

Article 9
Measures countering terrorist financing

(1) Terrorism represents one of the most serious forms of breaching values such as human dignity, freedom, equality and solidarity and respect for human rights and fundamental freedoms on which the European Union is founded. It also represents one of the most serious attacks on the principle of democracy and the principle of the rule of law, which are common to Member States and on which the European Union is founded. Act No 297/2008 prohibits the financing of terrorism and requires financial institutions to pay attention to transactions that may be related to terrorist financing.

(2) The issue of terrorist financing is also dealt with by the Financial Action Task Force (FATF) in its recommendations and further information and reports concerning terrorist financing are also published on the FATF website: (http://www.fatf-gafi.org/publications/fatfgeneral/documents/terrorist financing.html).

(3) The Act on the implementation of international sanctions (hereinafter also referred to as 'the International Sanctions Act') defines an international sanction as a restriction, order or ban in the regulations on international sanctions for the purposes of ensuring, maintaining and restoring international peace and security, the protection of fundamental human rights, the fight against terrorism and proliferation and achieving the objectives of the EU Common Foreign & Security Policy and the Charter of the United Nations Organisation. The aim of sanctions is to ensure, maintain or restore international peace and security, the fight against terrorism and proliferation according to the principles of the UN Charter and the EU Common Foreign & Security Policy.

(4) Procedure in fulfilling the reporting duty:

(a) in the framework of CFT, financial institutions apply toward customers procedures analogous to those applied in AML, including the reporting of unusual transactions connected with terrorist financing to the FIU;
(b) financial institutions are required to report unusual transactions to the FIU promptly (Article 17(1) of Act No 297/2008); Act No 297/2008 defines unusual transactions as, inter alia, a transaction in which there is a justified assumption that the customer or beneficial owner is a person against whom international sanctions have been imposed, or a person which may be in a relationship with that person, or as a transaction in which there is a reasonable assumption that the subject of it is or should be a thing or service that may relate to a thing or service against which sanctions are imposed under the International Sanctions Act;
(c) financial institutions are required to provide the Ministry of Finance of the Slovak Republic, within the terms set by it, with a list of customers subject to international sanctions under the International Sanctions Act and relevant decrees. The list also contains the account numbers and account balances of these customers (hereinafter referred to as 'persons subject to sanctions').

(5) A person subject to sanctions is a person against which an international sanction has been imposed and which may be:

(a) a state against which an international sanction has been imposed;

(b) a citizen of a state against which an international sanction has been imposed;
(c) a member or representative of a person against which an international sanction has been imposed;
(d) other natural person staying in the territory against which an international sanction has been imposed;
(e) a legal person domiciled in the territory against which an international sanction has been imposed, or
(f) a person included on the lists of persons subject to sanctions issued by Sanctions Committees of the United Nations Security Council, or a person determined in decisions taken in accordance with Title V of the Treaty of the European Union and in other EU legal acts.

(6) A list of persons subject to sanctions is a list of natural persons and legal persons against which international sanctions have been imposed in regulations on international sanctions published in the Official Journal of the European Union or in the Collection of Laws of the Slovak Republic. Lists of persons subject to sanctions form a part of the annexes to individual regulations and decisions of the EU, which obligate all financial institutions of Member States to immediately freeze financial and economic resources of persons subject to sanctions from states listed in the annexes to the individual regulations and decisions of the EU.

The EU regulations and decisions concerning exclusively persons subject to sanctions and comprehensive restrictive measures, including the consolidated list, which contains the names and identification data of all persons, groups and entities subject to financial restrictions of the EU Common Foreign & Security Policy (in the framework of enforcing the Common Foreign & Security Policy) are listed on the website (https://eeas.europa.eu/topics/sanctions-policy_en).

In this regard, the EU sanctions are listed on the website of the Ministry of Foreign Affairs of the Slovak Republic (https://www.mzv.sk/zahranicna-politika/medzinarodne-sankcie, http://eeas.europa.eu/cfsp/sanctions/docs/measures_en.pdf).

A consolidated list of sanctions is published on the website: (https://www.un.org/sc/suborg /en/sanctions/un-sc-consolidated-list).

(7) Inclusion of a person on and their exclusion from the list and the rights and obligations of persons included on the list of persons subject to sanctions are governed in Slovakia by the provisions of Articles 16 to 18 of the International Sanctions Act.

(8) A financial institution acts in accordance with the procedures for efficient implementation in practice of the rules of financial assets freezing of persons subject to sanctions in Slovakia which are published on the website (https://www.finance.gov.sk/sk/financie/financny-trh/bankovnictvo/sankcie-eu/).

Article 10
Archiving of data and documentation

(1) A financial institution is entitled, for the purposes of performing customer due diligence (Articles 10 to 12 of Act No 297/2008) also for the purposes of detecting unusual transactions (Article 14 of Act No 297/2008) and without informing and the consent of the customer concerned, to ascertain, acquire, record, store, use and otherwise process a customer's personal data and other information in accordance with the provisions of Article 10(1), Article 11(3) and Article 12 of Act No 297/2008.

(2) Under Article 88 of Act No 492/2009 a financial institution is entitled to acquire the necessary personal data also by copying, scanning or other recording of official documents on information media, as well as to process birth registration numbers and other data and documents without the customer's consent and in the scope set out in the mentioned provisions of Article 19(1) of Act No 297/2008.

(3) A financial institution stores (archives) data on the identification of customers and on the verification of identification, records on customers' products and services and financial transactions and records on ascertaining beneficial owners' identity, including photocopies of relevant documents.

(4) Under Article 19(1) and (2) of Act No 297/2008 a financial institution is required to archive for the period of five years:

(a) from the end of the contractual relationship with a customer, information and written documents acquired by way of the procedure under the provisions of Articles 10 to 12 and Article 14 of Act No 297/2008;

(b) from the provision of a product and service and the execution of a transaction, all data and written documents on the customer.

(5) In view of the importance of information acquired by the financial institution in fulfilling AML/CFT duties under Article 14(2)(a) of Act No 297/2008, it is necessary to archive in the statutory period (5 years from the written record being made) also written records referred to in paragraph 3 of the mentioned Article.

(6) A financial institution is required to archive this data and written documents also for longer than five years if the FIU requests it do so by way of a written request containing the period and scope of archiving data and written documents. This duty also applies to a financial institution that ceases business, up until the expiry of the period during which it is required to archive these data and written documents.

(7) A financial institution's procedure in archiving data and documentation, and records related to AML/CFT is governed by the Programme, which should, in accordance with the Act, specify in more detail the following:

(a) the records that need to be archived (at least data on customer identification and records on the customer's business transactions and financial transactions, including written records under Article 14(3) of Act No 297/2008 and data on identification of the beneficial owner);

(b) the form of records (paper, electronic);

(c) the place, method and period for which records are to be archived, taking account of

1. the end of the contractual relationship with the customer;
2. the customer's product and service or financial transaction execution, and
3. a written request of the FIU and the period determined (Article 19(3) of Act No 297/2008).

(a) records that need to be archived:

1. records on customer due diligence performed

A financial institution archives the data and written documents of customer due diligence performed (basic, simplified, enhanced) acquired in accordance with the provisions of Articles 10, 11 and 12 of Act No 297/2008, like the identification and verification of a customer's identity, identification of the beneficial owner, information on the purpose and intended nature of a product or service, identification of politically exposed persons or persons subject to

sanctions, ascertaining the origin of property and the source of funds depending on the AML/CFT risks.

2. records on customers' risk rating
Documents and information related to customers' assignment to risk groups must be archived. A financial institution records and archives any important information confirming circumstances justifying a customer's reassignment to a different risk group (and therefore a change of their risk profile), acquired through communication with a customer or otherwise, together with other information on the customer.

3. records on financial transactions
Internal regulations of a financial institution should establish the duty to record all products, services and financial transactions made for customers in the financial institution's accounting and reporting. Records on financial transactions that support accounting entries should be archived in a form that allows the FIU, supervisory authorities, control authorities and law enforcement authorities to compile a satisfactory record and to verify each customer's risk profile. Supporting records contain the customer's instructions related to the customer's financial transactions. The financial institution archives records on each financial transaction made by the customer, including one-off financial transactions. The archiving period in this case is the same as for archiving identification records and documentation.

4. records on internal notifications of unusual transactions and unusual transaction reports
A financial institution is required to archive all reports on customers' suspicious activities, namely internal notifications of unusual transactions intended for the Nominated Officer, as well as unusual transaction reports sent by the Nominated Officer to the FIU. If the Nominated Officer, after assessing the relevant information and knowledge concerning a customer's suspicious activity, decides that the activity does not constitute an unusual transaction and does not report it to the FIU, the reasons for that decision must also be recorded and archived together with the records on the particular business transaction.

5. records of staff training (education) conducted
A financial institution archives records on staff training, containing the date and content of the training and the confirmation that the respective employee attended the training and was familiarised with the financial institution's AML/CFT Programme, as well as the related internal regulations of the financial institution.

6. Programme
A financial institution archives the Programme, which contains information on statutory provisions, staff responsibilities and all operational procedures and duties of staff at the financial institution in the products and services provision and financial transactions execution, including the most frequent forms of unusual transactions.

7. records on inspections performed
A financial institution archives records on inspections performed.

(b) and (c) Form of records and place, method and period for which records must be archived

Originals or photocopies of paper documents and documentation, as well as data stored in personal computers and on mechanical media for electronic data must be archived. Archiving periods are the same, regardless of the form in which the data is archived.

In view of the need to additionally provide data on customers and customers' financial transactions, particularly for the FIU and law enforcement authorities, it is important that the financial institution is able to search, without delay, for the necessary documents (documentation and media) containing data and records.

A financial institution archives such information and documents also following the expiry of the statutory term for those customers and their financial transactions in the case of which an investigation has been started from the side of law enforcement authorities, or a criminal prosecution begun, and for the purposes of investigation and criminal prosecution, on the basis of a written request by the FIU pursuant to Article 19(3) of Act No 297/2008, in the scope and for the period stated in the request.

(8) Records prepared and archived by a financial institution should satisfy statutory requirements for record keeping on customer data and also enable:

(a) an independent party to evaluate the efficiency of compliance with basic principles, as well as the financial institution's AML/CFT procedures;
(b) reconstruction of the course of financial transactions made by the financial institution for a customer;
(c) identification and location of each customer;
(d) identification of all internal notifications of unusual transactions and external unusual transaction reports;
(e) fulfilment within a reasonable time of statutory requests by the FIU, supervisory authority and law enforcement authorities concerning a customer and a financial transaction.

Article 11
Ensuring the system and ensuring performance of internal control

(1) The system of control comprises a specification of control responsibilities at all levels of the management as well as the performance of control activity itself by:

(a) the financial institution's supervisory board;
(b) members of the financial institution's statutory body;
(c) the Nominated Officer (his deputy or the Prevention Unit);
(d) managerial staff;
(e) staff involved in the processing of customers' products and services and financial transactions;
(f) staff coming into contact with customers in entering into transactions or executing financial transactions;
(g) staff responsible for performing internal control, who is responsible for controlling all units, including the Nominated Officer, or Prevention Unit and relevant staff.

(a) and (b) Control performed by a financial institution's statutory body and supervisory board

Control is based on legislation of general application and the financial institution's internal regulations and derives from the position in the hierarchy of the financial institution's management system. The statutory body of a financial institution and Responsible Person of a branch evaluates regularly, at least once a year, the effectiveness of the existing system – the AML/CFT policy, the Programme and specific measures, including the activity of the relevant units and staff.

(c) and (d) Control activity performed by the Nominated Officer and managerial staff

Control activity is based on powers, duties and responsibilities of the Nominated Officer and all managerial staff of a financial institution and is performed as regular and ongoing controlling the performance of work duties, consisting in the verification and approval of the quality, level or state of the performance of the work activities of subordinate staff in the AML/CFT area.

(e) and (f) Control performed by staff

This represents an ongoing control process at various units of a financial institution performed on a daily basis. It comprises control mechanisms that are a direct component of staff's working procedures as well as their work duties, tasks and responsibilities in the first contact with customers, as arise from AML/CFT prevention.

(g) Control performed by staff responsible for performing internal control

Staff responsible for performance of internal control checks compliance with the Programme and internal regulations and verifies AML/CFT procedures adopted, as well as the performance of duties by staff, managerial staff and the Nominated Officer (his deputy or the Prevention Unit). The performance of control should be focused primarily on control of the Programme of own activity in the AML/CFT area (pursuant to Article 20 of Act No 297/2008), the financial institution's related internal regulations and on control of:

1. the methods of exercising customer due diligence (performance of the relevant degrees of customer due diligence);
2. procedures for ensuring that customer information received is up-to-date (verification);
3. assessment of specific financial transactions, monitoring of customers, their financial transactions and business relationships;
4. risk evaluation and management;
5. procedure for assessing unusual transactions; whether the overview of unusual transaction types is up to date; procedure for internal notification of unusual transactions and reporting of unusual transactions to the FIU;
6. the content, timetable and performance of staff training, and
7. records archiving.

(2) The annual plan of control activity carried out by staff responsible for performing internal control should include comprehensive control of the AML area and control of the Programme of own activity in the AML/CFT area at least once a year. Based on this inspection, staff responsible for performing internal control shall prepare a written report which shall include assessment of the AML area, information on identified shortcomings and draft measures for their rectification.

In the framework of regular verification of a financial institution's AML/CFT system and processes, the functionality, effectiveness and efficiency of all elements, tools, procedures, management and control mechanisms applied in this area should be evaluated. Members of the statutory body and supervisory board of a financial institution and head of a branch should be regularly informed of the results of controls performed, at minimum once a year and immediately in the case of finding serious shortcomings.

PART III.
Final provision

This Methodological Guideline replaces in full the Methodological Guideline No 9/2012 of the Financial Market Supervision Unit of Národná banka Slovenska of 20 November 2012 regarding the prevention by banks and foreign bank branches of money laundering and terrorist financing.

Vladimír Dvořáček
Member of the Bank Board and
Executive Director
of the Prudential Supervision Division
of the Financial Market Supervision Unit
of Národná banka Slovenska

Júlia Čillíková
Executive Director of the
Financial Consumer Protection
and Regulation Division
of the Financial Market Supervision Unit
of Národná banka Slovenska

ANNEX 1

Guidelines on risk factors relating to customer relationships and occasional transactions

This annex is based on Annex 2 to Act No 297/2008 Coll. and provides more detailed guidance on risk factors financial institutions should consider when performing customer due diligence for AML purposes.

These guidelines have been prepared in accordance with Joint Guidelines under articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced 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 (JC 2017 13) (hereinafter the 'joint guidelines').

In relation to risk factors, financial institutions should also adjust the extent of their obligatory customer due diligence measures in a way that is commensurate to the identified money laundering and terrorist financing risks.

The joint guidelines are available at the following address: (https://esas-joint-committee.europa.eu/Publications/Guidelines/Guidelines%20on%20Risk%20Factors_SK_04-01-2018.pdf).

Part 1
General guidelines on assessing and managing risk

'Risk factors' means variables that, either on their own or in combination, may increase or decrease the money laundering and terrorist financing (hereinafter 'ML/TF') risk posed by an individual business relationship or occasional transaction.

Financial institutions should perform a business-wide assessment of ML/TF risks to understand where they are exposed to ML/TF risk and which areas of their business they should prioritise in the mitigation of these risks. In line with Annex 2 to Act No 297/2008 Coll. and Article 8 of Directive (EU) 2015/849, financial institutions should identify and assess the ML/TF risks associated with their products and services, customers, and transactions and delivery channels used to service their customers. The steps taken by the financial institutions to identify and mitigate the ML/TF risks shall be proportionate to their nature and size.

Financial institutions should adjust the extent of initial customer due diligence measures on a risk-sensitive basis. Where the risk associated with a business relationship has been assessed as low, financial institutions shall apply simplified customer due diligence measures. Where the risk associated with a business relationship has been assessed as higher, financial institutions shall apply enhanced customer due diligence measures.

Financial institutions should collect adequate information in order to establish that they identified and assessed all risk factors with the objective of conducting a comprehensive assessment of risks associated with a particular business relationship or occasional transaction.

When assessing and managing risks, financial institutions should always consider the following sources of information:

32 / 52

(a) the European Commission's supranational risk assessment (under Article 6 of Directive (EU) 2015/849);

(b) information from the national risk assessment (under Article 7 of Directive (EU) 2015/849), policy statements, alerts and explanatory memorandums to relevant legislation;
(c) information from regulators, such as guidance, statements, etc.;
(d) information from the FIU, such as threat reports, alerts and typologies;
(e) information obtained as part of the customer due diligence process.

In addition to the sources mentioned above, financial institutions should consider, among others, the following sources of information:
(a) own knowledge and expertise acquired during the provision of services to their customers;
(b) information from industry bodies, such as typologies and information on emerging risks;
(c) information from civil society, such as corruption indices, country reports, etc.;
(d) information from international standard-setting bodies in the field of AML/CFT (FATF, MONEYVAL), such as reports on mutual evaluation of ML/TF risks;
(e) information from other credible and reliable open sources, such as media, the Internet, etc.;
(f) information from statistical organisations and academia.

Part 2
Risk assessment

A risk assessment conducted by a financial institution should consist of two distinct but related steps:
2.1. the identification of ML/TF risks;
2.2. the assessment of ML/TF risks.

2.1. Identification of ML/TF risks

When identifying ML/TF risks associated with a business relationship or occasional transactions, financial institutions should consider relevant risk factors related to:
(a) their customers;
(b) products, services and transactions requested by their customers;
(c) the countries or geographical areas their customers operate in;
(d) the delivery channels used by the financial institutions to deliver products, services and transactions.

Information about these ML/TF risk factors should come from a variety of sources. Financial institutions should determine the number of these sources on a risk-sensitive basis.

2.1.1. Customer risk factors

When identifying the risks associated with their customers, including their customer's beneficial owners, financial institutions should consider the risks related to:

(a) the customer's and the customer's beneficial owner's business or professional activity

Risk factors that may be relevant when considering the customer's business or professional activity include:

- Does the customer or beneficial owner have links to sectors that are commonly associated with higher corruption risk (such as construction, healthcare, the arms trade and defence, the extractive industries, public procurement, etc.)?
- Does the customer or beneficial owner have links to sectors that are associated with higher ML/TF risk (such as casinos, gambling venues or dealers in precious metals)?
- Does the customer or beneficial owner have links to sectors that involve significant amounts of cash?
- Does the customer have political connections (for example, are they a politically exposed person or is their beneficial owner a politically exposed person, do they have any links to a politically exposed person)?
- Does the customer or beneficial owner hold another prominent position or enjoy a high public profile that might enable them to abuse this position for private gain (for example, are they members of local or regional decision-making bodies with the ability to influence the awarding of public contracts, decision-making members of high-profile sporting bodies or individuals who are known to influence the government and other senior decision-makers)?
- Based on publicly available sources, is there evidence that the customer has been subject to sanctions for failure to comply with AML/CFT obligations?

(b) the customer's and the customer's beneficial owner's good repute

When considering the risks associated with the customer's good repute, financial institutions should consider the following factors:

- Are there adverse media reports or other relevant sources of information about the customer (for example, are there any allegations of criminality or terrorism against the customer)?
- Has the customer, beneficial owner or anyone known to be closely associated with them had their assets frozen due to administrative or criminal proceedings or allegations of terrorism or terrorist financing?
- Does the financial institution know if the customer or beneficial owner has been the subject of an unusual transactions report in the past?

(c) the customer's and the customer's beneficial owner's nature and behaviour

When considering the behaviour of their customers, financial institutions should note that not all of the risk factors below will be apparent at the outset of a business relationship and that they may emerge only once a business relationship has been established:

- Is the customer's ownership and control structure transparent and does it make sense? If not, is there an obvious lawful or economic rationale to this?
- Is there a sound reason for changes in the customer's ownership and control structure (such as sale or transfer of the company or a part thereof to other beneficial owners, etc.)?
- Does the customer request transactions that are complex, unusually large or have an unusual or unexpected pattern without an apparent economic or lawful purpose or a sound commercial rationale (for example, there are grounds to suspect that the customer is trying to evade specific thresholds set out for occasional transactions, etc.)?
- Does the customer request unnecessary or unreasonable levels of secrecy? Is the customer reluctant to share customer due diligence information, or does the customer appear to want to disguise the true nature of their business (for example when the customer requests private banking services)?
- Does the customer issue bearer shares as part of their business activity?

- Is the customer able to plausibly explain the source of their wealth or the source of funds (for example through their occupation, business activity, inheritance, donation or investments)?
- Does the customer use the products and services they have taken out when the business relationship was first established as expected and in line with the information obtained by the financial institution regarding the purpose and intended nature of the relationship?
- Are there indications that the customer might seek to avoid the establishment of a business relationship (for example by requesting only one transaction or several one-off transactions even where the establishment of a business relationship might make more economic sense)?

2.1.2. Products, services and transactions risk factors

When identifying the risks associated with their products, services or transactions, financial institutions should consider the risks related to the level of transparency the product, service or transaction affords, as well as the overall complexity, value or size of the product, service or transaction.

(a) risks related to the level of transparency the product, service or transaction affords:
The products, services and transactions allow the customer or beneficial owner to remain anonymous, or facilitate hiding their identity (such as bearer shares or activities of legal entities that can be structured in such a way as to take advantage of anonymity and allow dealings with shell companies).

(b) risks related to the complexity of the product, service or transaction:
Third party that is not part of the business relationship is able to give instructions for the execution of a transaction, product or service (for example in the case of certain correspondent banking relationships).
The transaction is complex and involves multiple parties or multiple jurisdictions (for example in the case of certain trade finance transactions). There are risks associated with financial institution's new products or services, in particular where this involves the use of new technologies (such as remote identification and verification of the customer without the customer being physically present).

(c) risks related to the value or size of the product or service:
The products or services are cash intensive (such as payment services), they facilitate high-value transactions and/or there are no caps on cross-border and cash/cashless transactions.

(d) risks related to the sector:
Do the products or services primarily concern the intermediation of virtual currency transactions and FX (foreign exchange) transactions, or the intermediation of gambling?

2.1.3. Customer's geographical area risk factors

When identifying risk associated with countries and geographical areas, financial institutions should consider the risks related to countries in which the customer or beneficial owner are based, which are their main places of business, and to which they have relevant personal links.

When identifying the geographical risk factors, financial institutions should also consider the overall effectiveness of a country's AML/CFT regime. This includes the following risk factors:

The country has been identified by the European Commission as having strategic deficiencies in its AML/CFT regime, in line with Article 9 of Directive (EU) 2015/849. Where financial institutions deal with natural or legal persons resident or established in third countries that the Commission has identified as presenting a high ML/TF risk, they must always apply enhanced customer due diligence measures.

There is information from a credible and reliable source about the quality of the country's AML/CFT controls, including information about the quality and effectiveness of regulatory enforcement and financial sector oversight. Examples of possible sources include the FATF mutual evaluation reports, the FATF's list of high-risk and non-cooperative countries, International Monetary Fund (IMF) assessments, etc. When assessing the risks, financial institutions should note that the country's membership in the FATF or FSRB (e.g. MoneyVal) does not, of itself, mean that the country's AML/CFT regime is adequate and effective.

There is information from credible and reliable public sources about the level of predicate offences to money laundering, for example corruption, organised crime, tax crime, etc. Examples include corruption perceptions indices, OECD country reports on the implementation of the OECD's anti-bribery convention, and the United Nations Office on Drugs and Crime World Drug Report.

There is information suggesting that the country provides funding or support for terrorist activities or that groups committing terrorist offences are known to be operating in the country.

The country is subject to financial sanctions or embargoes that are related to terrorism, financing of terrorism or proliferation issued by the United Nations or the European Union.

2.1.4. Delivery channel risk factors

When identifying the risks associated with the way in which the customer establishes business relationships, financial institutions should consider the following risk factors:

https://www.mfsr.sk/sk/media/tlacove-spravy/vysledky-zasadnutia-centra-financne-inovacie.html.

The customer has been introduced by another institution of the same financial group. The financial institution should consider to what extent can it rely on this introduction as reassurance that the customer will not expose the financial institution to excessive ML/TF risk? The financial institution should verify whether the other institution of the same financial group applies obligatory customer due diligence measures to EU standards in line with Article 28 of Directive (EU) 2015/849.

The customer has been introduced by a third party, for example by a bank that is not part of the same group, and the third party is a financial institution (the financial institution should verify how does the third party apply customer due diligence measures, how does it keep records and whether it is supervised for compliance with comparable AML/CFT obligations).

The customer has been introduced through a tied agent, that is, without direct financial institution contact (the financial institution should verify whether the agent has obtained enough information so that the financial institution knows its customer and the level of risk associated with the business relationship).

The financial institution cooperates with an intermediary whose level of compliance with applicable AML/CFT legislation might be inadequate.

2.2. Assessment of ML/TF risks

Financial institutions should take a holistic view of the ML/TF risk factors they have identified that, together, will determine the level of ML/TF risk associated with a business relationship or occasional transactions. As part of this assessment, financial institutions may decide to weigh factors differently depending on their importance.

When weighting risk factors, financial institutions should make an informed judgement about the relevance of different risk factors in the context of a business relationship or occasional transaction.

When weighting risk factors, financial institutions should ensure that:
(a) weighting is not unduly influenced by just one factor identified;
(b) economic or profit considerations do not influence their risk rating;
(c) weighting does not lead to a situation where it is impossible for any business relationship to be classified as high risk;
(d) they are able to over-ride any automatically generated risk scores where necessary. The rationale for the decision to over-ride such scores should be documented appropriately.

During the assessment process, financial institutions should assign higher weight to material risk factors and lower weight to non-material risk factors.

Following their risk assessments, financial institutions should categorise their business relationships and occasional transactions according to the perceived level of ML/TF risk.

Financial institutions should decide on the most appropriate way to categorise risk. This will depend on the complexity and size of the financial institution and the types of ML/TF risk it is exposed to. Financial institutions are recommended to use the following three risk categories:
(a) High;
(b) Medium;
(c) Low.

Financial institutions may use a more detailed categorisation, for example by splitting the “Medium risk” category into “Medium low risk” and “Medium high risk”, etc.

Part 3
ML/TF risk management, simplified and enhanced customer due diligence, risk monitoring and review

Risk assessment should help financial institutions determine their risk management priorities in the AML/CFT field. Financial institutions should set their obligatory customer due diligence measures to a level that is appropriate considering the identified ML/TF risks.

3.1. Simplified customer due diligence

To the extent allowed by Act 297/2008 Coll., financial institutions may apply simplified customer due diligence measures in situations where the ML/TF risk associated with a business relationship has been assessed as low. Simplified customer due diligence is not an exemption from any of the customer due diligence measures. Financial institutions may adjust the amount, timing or type of each or all of the customer due diligence measures in a way that is commensurate to the low risk they have identified.

Simplified customer due diligence measures financial institutions may apply include:

3.1.1. adjusting the timing of customer due diligence, for example where the products, services or transactions sought have features that limit their use for ML/TF purposes, for example by:

1) verifying the customer's or beneficial owner's identity during the establishment of the business relationship;
2) verifying the customer's or beneficial owner's identity once transactions exceed a defined threshold or once a reasonable time limit has lapsed.

Financial institutions must make sure that:

(a) this does not result in an exemption from obligatory customer due diligence, that is, financial institutions must ensure that the customer's or beneficial owner's identity will ultimately be verified;
(b) the threshold or time limit is set at a reasonably low level (although, with regard to terrorist financing, financial institutions should note that a low threshold alone may not be enough to reduce risk);
(c) they have systems in place to detect when the threshold or time limit has been reached;
(d) they do not defer obligatory customer due diligence or delay obtaining relevant information about the customer.

3.1.2. adjusting the quantity of information obtained for identification, verification or monitoring purposes, for example by:

1) verifying identity on the basis of information obtained from one reliable, credible and independent document only; or
2) assuming the nature and purpose of the business relationship.

3.1.3. adjusting the quality or source of information obtained for identification, verification or monitoring purposes, for example by:

1) accepting information obtained from the customer rather than an independent source when verifying the beneficial owner's identity; or
2) where the risk associated with all aspects of the relationship is low, relying on the source of funds to meet some of the obligatory customer due diligence requirements (for example where the funds are state benefit payments).

3.1.4. adjusting the frequency of obligatory customer due diligence updates and reviews of the business relationship (for example carrying these out only when trigger events occur such

as the customer looking to take out a new product or service or when a certain transaction threshold is reached).

3.1.5. adjusting the frequency and intensity of transaction monitoring (for example by monitoring transactions above a certain threshold only). Where financial institutions choose to do this, they must ensure that the threshold is set at an appropriate level and that they have systems in place to identify linked transactions that, together, would exceed that threshold.

Financial institutions should ensure that the information they obtain when applying simplified customer due diligence measures are sufficient to justify the low risk. It must also be sufficient to give the financial institutions enough information about the nature of the business relationship to identify any unusual or suspicious transactions. Simplified customer due diligence does not exempt a financial institution from reporting unusual transactions to the FIU.

3.2. Enhanced customer due diligence

Financial institutions must apply enhanced customer due diligence in higher risk situations to manage and mitigate those risks appropriately. Enhanced customer due diligence measures cannot be substituted for regular obligatory customer due diligence measures but must be applied in addition to them.

Under Article 12 of Act 297/2008 Coll., financial institutions are obliged to perform enhanced customer due diligence where risk assessment under Article 10(4) of Act 297/2008 Coll. indicates that a customer, a type of product or service or an individual product or service poses a higher ML/TF risk. Financial institutions must **always** perform enhanced customer due diligence:

3.2.1. where the customer is a politically exposed person;

3.2.2. with respect to cross-border correspondent relationship of a bank and financial institution with respondents from third countries;

3.2.3. where they deal with natural persons or legal entities established in countries that the European Commission has identified in Commission Delegated Regulation (EU) 2016/1675 as presenting a high risk (specific enhanced customer due diligence measures apply).

3.2.1. Enhanced due diligence with respect to politically exposed persons

Financial institutions that have identified that a customer or beneficial owner is a politically exposed person **must always**:

(a) Take adequate measures to establish the source of wealth and the source of funds in order to allow them to satisfy themselves that it does not handle the proceeds from criminal activity. The measures financial institutions should take to establish the politically exposed person's source of wealth and the source of funds will depend on the degree of risk associated with the business relationship. Financial institutions should verify the source of wealth and the source of funds on the basis of reliable and independent data, documents or information.

(b) Obtain approval of the statutory body or Nominated Officer under Article 20(2)(h) of Act 297/2008 Coll. for establishing, or continuing, a business relationship with a politically exposed person. The appropriate level of seniority for sign-off should be determined by the level of increased risk associated with the business relationship, and the senior manager approving a business relationship with a politically exposed person should have sufficient

seniority and oversight to take informed decisions on issues that directly impact the risk profile of the financial institution as a whole. When considering whether to approve a relationship with a politically exposed person, senior management should base their decision on the level of ML/TF risk the financial institution would be exposed to if it entered into that business relationship. The financial institution should also consider how well equipped it is to manage and mitigate that risk effectively.

(c) Apply enhanced ongoing monitoring of both transactions and the risk associated with the business relationship. Financial institutions should identify unusual transactions and regularly review the information they hold to ensure that any new or emerging information that could affect the risk assessment is identified in a timely fashion. The frequency of ongoing monitoring should be determined by the level of risk associated with the relationship.

Financial institutions must apply all of these measures to politically exposed persons, their family members and known close associates. They should adjust the extent of these measures on a risk-sensitive basis. Financial institutions should apply these measures for a period of at least 12 months after the termination of the term of significant public office that the politically exposed person held, at minimum, however, until the financial institution does not rule out the risk specific for politically exposed persons.

3.2.2. Enhanced customer due diligence with respect to correspondent relationships

Financial institutions must take specific enhanced customer due diligence measures where they have a cross-border correspondent relationship with a respondent who is based in a third country.

Financial institutions must make sure that they:

(a) collect information on the partner institution in order to determine the nature of their business and their good repute and to ascertain the level of effectiveness of supervision using information from public sources;

(b) assess the partner institution's AML/CFT controls;

(c) obtain approval of the statutory body or Nominated Officer under Article 20(2)(h) of Act 297/2008 Coll. for establishing a new correspondent relationship;

(d) verify that the partner institution is authorised to perform its business activities;

(e) establish, in the case of account-based payments, whether the partner institution verified the identity of the customer who has direct access to the partner institution's account and performed basic customer due diligence, and whether the partner institution is able, if requested, to provide the information in the extent of basic customer due diligence.

3.2.3. Enhanced customer due diligence with respect to high-risk third countries and high-risk situations

High-risk third countries:

When dealing with customers established or residing in a high-risk third country identified by the Commission in Commission Delegated Regulation (EU) 2016/1675 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies, and in all other high-risk situations, financial institutions should take an informed decision about which enhanced customer due diligence measures are appropriate for each high-risk situation.

Financial institutions are not required to apply all the enhanced customer due diligence measures listed below in all cases. For example, in certain high-risk situations it may be appropriate to focus on enhanced ongoing monitoring of the business relationship. During supervision, the obliged entity shall demonstrate that the extent of performed customer due diligence is commensurate with the identified level of ML/TF risk.

Complex and unusually large transactions:

Financial institutions should put in place adequate procedures to detect unusual transactions or patterns of transactions. Where a financial institution detects transactions that are unusual because:

(a) they are larger than what the financial institution would normally expect based on its knowledge of the customer, the business relationship or the category to which the customer belongs;

(b) they have an unusual or unexpected pattern compared with the customer's normal activity or the pattern of transactions associated with similar customers or deals; or

(c) they are very complex compared with other, similar, transactions associated with similar customer types, products or services, and the financial institution is not aware of an economic rationale or lawful purpose or doubts the veracity of the information it has been given.

These enhanced customer due diligence measures should be sufficient to help the financial institution determine whether these transactions give rise to suspicion and must at least include:

(a) taking reasonable and adequate measures to understand the background and purpose of these transactions, for example by establishing the source and destination of the funds or finding out more about the customer's business to ascertain whether the customer would be making such transactions; and

(b) monitoring the business relationship and subsequent transactions more frequently and with greater attention to detail. A financial institution may decide to monitor individual transactions where this is commensurate to the risk it has identified.

Enhanced customer due diligence measures should in particular include:

(a) **Increasing the quantity of information** obtained for customer due diligence purposes, for example:
   1) identifying the customer using additional documents, obtaining information about the customer's ownership and control structure, obtaining information about the customer's family members and close business partners, and obtaining information about the customer's and beneficial owner's past and present business activities;
   2) obtaining more detailed information about the purpose and intended nature of the business relationship with the customer, for example information about the number, size and frequency of transactions that are likely to pass through the payment account, and information about the nature of the customer's and beneficial owner's business, to enable the financial institution to better understand the nature of the business relationship;

(b) **Increasing the quality of information** obtained for obligatory customer due diligence purposes, for example:
   1) requiring the first payment to be carried out through an account verifiably in the customer's name, where the customer presented a document proving the existence of such account;
   2) establishing that the customer's wealth and the funds that are used in the business relationship are not the proceeds of criminal activity and that the source of wealth and

source of funds are consistent with the financial institution's knowledge of the customer and the nature of the business relationship;

(c) **Increasing the frequency of reviews** to be satisfied that the financial institution continues to be able to manage the risk associated with the individual business relationship, for example by:
   1) increasing the frequency of regular reviews of the business relationship to ascertain whether the customer's risk profile has changed and whether the risk remains manageable for the financial institution;
   2) conducting more frequent and in-depth transaction monitoring to identify any unexpected transactions that might give rise to suspicion of ML/TF. This may include establishing the destination of funds or ascertaining the reason for certain transactions;
   3) obtaining the approval of the statutory body or a senior manager or the Nominated Officer to establish or continue the business relationship to ensure that senior management are aware of the risk their financial institution may be exposed to.

Other considerations with respect to enhanced due diligence

Financial institutions should not enter into a business relationship if they are unable to comply with their obligatory customer due diligence requirements, if they are not satisfied that the purpose and nature of the business relationship are legitimate or if they are not satisfied that they can effectively manage and mitigate the risk that they may be used for ML/TF purposes. Where such a business relationship already exists, financial institutions should terminate it or suspend transactions of the customer until it can be terminated.

Financial institutions should note that the application of a risk-based approach does not of itself require them to refuse, or terminate, business relationships with entire categories of customers that they associate with higher ML/TF risk, as the risk associated with individual business relationships will vary, even within one risk category.

Where financial institutions have reasonable grounds to suspect that ML/TF is being attempted, they must report this to their FIU.

3.3. Risk monitoring and review

Financial institutions should keep their assessments of the ML/TF risks associated with individual business relationships and occasional transactions as well as of the underlying factors under review to ensure their assessment of ML/TF risk remains up to date and relevant.

Financial institutions should also ensure that they have systems (including a system to set a date on which the next risk assessment will take place) and controls in place to identify emerging ML/TF risks. They should also be able to assess these risks and incorporate them into their risk assessment. Any update to a risk assessment and adjustment of accompanying customer due diligence measures should be proportionate to the identified ML/TF risk.

Systems and controls to monitor and review risks that financial institutions should put in place include:

(a) processes to ensure that internal risk information is reviewed regularly to identify trends and emerging issues, in relation to both individual business relationships and the financial institution's business;

(b) processes to ensure that the financial institution regularly reviews information sources (such as the national risk assessment report, EU supranational risk assessment report, report of the Financial Intelligence Unit, other national regulators, own knowledge and analysis, etc.);

(c) processes to ensure careful recording of issues that could have a bearing on risk assessment (such as internal suspicious transaction reports, compliance failures and intelligence from front office staff).

Financial institutions should record and document their risk assessments of business relationships, as well as any changes made to risk assessments as part of their reviews and monitoring, to ensure that they can demonstrate to the competent authorities that their risk assessments and associated measures to manage and mitigate risks are adequate.

Part 4
Sectoral guidelines for electronic money issuers – Risk factors

The level of ML/TF risk associated with electronic money depends primarily on the features of individual electronic money products and the degree to which electronic money issuers use other persons to distribute (hereinafter 'distributors') and redeem electronic money on their behalf.

Electronic money institutions should consider the following risk factors and measures alongside those set out above.

4.1 Products, services and transactions risk factors:

(a) the product or service places no restrictions on cash and cashless transactions;
(b) the product or service allows high or unlimited amount of funds to be stored on the electronic money account/product (medium);
(c) the product or service allows anonymous loading of electronic money;
(d) the product or service can be funded with payments from unidentified third parties.

4.2 Customer risk factors

(a) the customer uses the medium loaded with electronic money together with several other people whose identity is not known to the electronic money issuer;
(b) there are frequent changes in the customer's identification data related to the payment medium used to store electronic money (such as home address or IP address);
(c) the customer does not use the payment medium loaded with electronic money for the purpose it was issued for.

4.3. Delivery channel risk factors:

(a) financial institutions rely on a third party's obligatory customer due diligence measures in situations where they do not have a long-standing relationship with the referring third party;
(b) new delivery channels (such as distribution through intermediaries who do not have sufficient measures implemented) which have not yet been sufficiently tested.

4.4. Country and geographical area risk factors

(a) the customer's funds are derived from personal or business links to jurisdictions associated with higher ML/TF risk;
(b) the payee is located in a jurisdiction associated with higher ML/TF risk; financial institutions should pay particular attention to jurisdictions known to provide funding or support for terrorist activities or where groups committing terrorist offences are known to be operating, and jurisdictions subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation.

Part 5
Sectoral guidelines for money remitters – Risk factors

For the purposes of these guidelines, 'money remitters' are payment institutions that have been authorised to provide this payment service.

Financial institutions (money remitters) should consider the following risk factors and measures alongside those set out above.

5.1. Products, services and transactions risk factors

(a) the product or service allows high-value or unlimited-value transactions;
(b) the product or service has a global reach;
(c) transactions are made from one or more payers in different countries to a local payee.

5.2. Customer risk factors

(a) the customer is a cash-intensive undertaking;
(b) the customer is acting for someone else;
(c) the customer's behaviour makes no apparent economic sense (for example the customer accepts a poor exchange rate or high charges, requests a transaction in a currency that is not a commonly used tender, etc.);
(d) the customer does not use the product or service for the purpose it was designed for;
(e) the customer appears to know little or is reluctant to provide information about the payee.

5.3. Delivery channel risk factors

(a) there are no restrictions on the funding of the medium loaded with electronic money;
(b) the delivery channel used provides a degree of anonymity;
(c) the service is provided online without adequate safeguards;
(d) the money remittance service is provided through agents that represent more than one principal, have an unusually high turnover or execute an unusually high number of transactions, etc.

5.4. Country and geographical area risk factors

(a) the payer or the payee is located in a jurisdiction associated with higher ML/TF risk;
(b) the payee is resident in a jurisdiction that has a less developed financial sector.

ANNEX 2

Forms and methods of money laundering and terrorist financing, and indicators for detecting unusualness

Detection and assessment of UTs, their analysis, processing and subsequent reporting to the FIU is a purposeful and systematic process that, with the concurrent application of the KYC principle, forms the basis for competent detection of the signs of unusualness on the basis of information available to the financial institution's Nominated Officer at the time of assessing products, services, transactions or other acts, or on the basis of information that they can acquire within a time that does not jeopardise the reporting of a UT within the statutory period.

When assessing a product, service, transaction and business relationship, it is necessary to take particular account of:

1. Information on the customers and circumstances of concluding the business relationship, or circumstances of the product or service provided, or transaction conducted, from the financial institution's front office staff;
2. Internal reports of UTs and records on them;
3. Information acquired in the course of the ongoing monitoring of the business relationship;
4. Information acquired in the course of the retrospective assessment of the customer's products, services and transactions;
5. Compilation reports and outputs from the financial institution's internal information system, which should contain an analytical tool for automatic evaluation and identification of signs indicating possible UTs, and which must be harmonised with the Programme;
6. Information received from other obliged entities;
7. Information from commercial databases;
8. Information from open sources;
9. Information arising from requests and instructions of authorised entities, in particular the police force, prosecutor, courts, executors, etc.;
10. Information from the FIU, in particular feedback on the effectiveness of UT reports received and the manner of their handling, and warnings and information on indicators and new forms of UTs published or targeted by the FIU;
11. Analyses and investigation results from AML unit staff.

When analysing and assessing products, services and transactions with the aim of determining whether they do or do not constitute a UT, it is necessary to always assess them particularly in terms of:

1. The person making or requesting the provision of product, service or transaction;
2. The legal person which, in the case that it does not act on its own behalf, is owned by, represented by, acted for by, or in any other way represented by such person;
3. The product, service, transaction and requests of the customer;
4. Other available and known relationships, circumstances and information acquired not only through the activity of the financial institution and its staff, but also through the activity of, e.g., competent authorities;
5. Decisions on a potential delay of UTs.

When detecting and assessing UTs, AML staff and front office staff should take particular care to assess:

1. **Customer (natural person), focusing particularly on their:**

- Social status;
- Age (especially young and also old age are risk factors);
- Nationality (in the case of foreigners identify the reasons for product, service and transaction execution in Slovakia, whether they are nationals of a country supporting international terrorism, etc.);
- Position as a politically exposed person (PEP);
- Risk of corruption (persons with decision-making powers, representatives of public authorities);
- Criminal activities – ascertained from commercial databases and open sources whether the person has not been prosecuted or convicted for committing a crime, is suspected of a crime, suspected of affiliation to a criminal or terrorist group; a valuable source of such information, besides commercial databases and open sources, consists in requests and instructions from the police force, prosecutor and courts. The use of commercial databases is recommended with regard to the subject and scope of the financial institution's activity and application of customer due diligence;
- Debts toward third parties (credit register, tax debts, debts toward the Social Insurance Agency);
- Positive record in the obliged entity's registers (UT register, rejected products, services and transactions, fraud, etc.);
- Feedback and information from the FIU;
- External signs indicating affiliation to extremist groups and movements;
- Documents (a homeless person, person deprived of legal capacity, suspicion of altered or falsified documents, lost documents);
- Presence of third parties entering into the customer-financial institution relationship, or if it is clear that their presence is connected with the customer's conduct (the third party reluctant to present their identification or to provide more detailed relevant information);
- Communication, requirements and behaviour, knowledge of products, services, transactions and business activities, etc.

2. **Legal person, in the case of which it is necessary to analyse in particular:**

- The line of business in relation to the assessed product, service or transaction, as well as in terms of creating the customer's risk profile;
- Determining whether the legal person is an obliged entity;
- The form and statute of the legal person;
- The date and place of registration in relation to the increased level of risk (name-plate company, virtual registered office and address, risk areas, etc., newly-established companies with an excessively high turnover);
- Company shareholders, statutory representatives, persons authorised to act, beneficial owners – applies similarly for each legal or natural person separately;
- Former company shareholders and statutory representatives (frequent changes in the legal person's statutory body);
- Course of business to date;
- Frequent changes of the company's registered address and name;
- Available information from open sources (lists of VAT entities stating the amount of excess tax deduction and the amount of tax payable, off-shore databases, etc.);
- Unpaid obligations toward business partners and the state (tax arrears);
- Information from credit and other available registers;
- Business partners;

- Misuse and risk of misuse for criminal activity;
- Positive record in the obliged entity's registers (UT register, rejected products, services and transactions, fraud, etc.).

3. Product, service and transaction (its form, method of execution and value), in the case of which it is necessary to focus particularly on:

- Legal and natural persons performing the product, service or transaction;
- Plausibility of the product, service or transaction and its purpose (transaction chains without an obvious economic and legal purpose);
- Degree of risk inherent in the product, service or transaction (cash implies a higher risk degree, transactions related to tax havens);
- Value and volume of the product, service or transaction (its value/volume is clearly disproportionate to the customer's previous regime);
- Subject of the product, service or transaction (transactions related to high risk commodities);
- Method and form of payment;
- Documents presented by the customer;
- Customer's requirements;
- Business partners (more companies suspect of carousel fraud, transaction chains),
- Information on similar products, services or transactions from open sources;
- Comment on the product, service or transaction from the financial institution's competent and expert units;
- Experience of other obliged entities with the given type of product, service or transaction.

Each financial institution shall determine the forms and methods of UTs according to its own criteria, taking account particularly of the scope and type of activities and services that it provides, its clientele, number of branches and places of operation, experience to date, as well as within the group of which it is a member.

Indicators of unusualness

In relation to a natural person:

- Persons in the case of whom it may be presumed that they do not act on their own behalf and may be directed by another person, i.e. a "money mule", and persons in the case of whom the risk of money laundering and terrorist financing is higher than that in the general population. Such persons can be recognised in particular on the basis of the following external characteristics and features:
- Unkempt appearance, poor social situation;
- Influence of narcotics;
- Ignorance of the product, service, transaction or line of business;
- Unusual and abnormal behaviour;
- Homeless persons with registered permanent residence only at a local authority office; the street name is missing in documents, or this fact is known to the financial institution employee;
- Persons who feature as the owner of several companies that have progressively been transferred to these persons over some time;
- Persons who, while being the true owner or executive of a company, nonetheless do not have disposal rights to the accounts or never act alone;
- The presence of third persons who direct or monitor the actions of such person;

- Persons using lost, falsified or altered documents;
- Persons intentionally giving false data, particularly on employment, place of residence, activities, etc.; also persons not responding to the financial institution's requests,
- Persons sought by police;
- Persons suspected of committing crime;
- Persons known or suspected to be a member of a criminal group;
- Persons on wanted lists of armed and intelligence services;
- Persons on lists of persons subject to sanctions,
- Persons on lists of terrorists or sympathisers of terrorism as such;
- Persons expressing through their appearance, behaviour or statements sympathy for extremism;
- Foreigners with no apparent relationship to Slovakia;
- Foreigners from areas known to be high-risk in relation to the promotion of international terrorism;
- Persons deprived of legal capacity;
- Children, youths, close to the age of a youth, and also elderly people;
- Persons with an increased risk of corruption – public administration representatives, representatives of political parties;
- Politically exposed persons, foreign public officials;
- Representatives of foundations, non-profit associations, etc.;
- Persons who have been the subject of a UT report;
- Persons registered as non-payers and unreliable persons according to registers and information available to the financial institution's staff;
- Persons engaged in the trade and production of goods and technology subject to control by the state and international community. Likewise, in terms of the risk of money laundering and terrorist financing, staff shall also assess persons who are close to such persons or about whom it is known that they act jointly or benefit from the actions of such persons.

In principle it does not apply that if a product, service, transaction or any act is performed by such a person this must automatically constitute a UT. It is always necessary to take a comprehensive view in assessing the actions of such persons.

In relation to a legal person:

- In respect of the legal person there acts on behalf of it, owns it, or its beneficial owner in any demonstrable relationship is a natural person who poses an increased risk of money laundering or terrorist financing;
- The legal person's registered line of business does not correspond to its real business;
- The line of business is high-risk in terms of the potential for money laundering – in particular gambling and bureaus de change;
- The line of business requires a special permit;
- Unclear ownership structure;
- The legal person, its owner or partner, is domiciled in a tax haven or area risky in terms of supporting and financing terrorism;
- The legal person has only a virtual registered office;
- A name-plate company;
- Other obliged entity – the tendency to not devote attention to the transactions of other obliged entities;
- A legal person that trades with other legal persons posing a risk of money laundering or

terrorist financing;

- A legal person whose trade name or line of business is misleading and suggests that it may be a bank, financial institution, etc.;
- A legal person about which the financial institution knows from available registers that it is a debtor or fails to meet tax obligations;
- A legal person about which it is known that it has been misused or involved in any other way whatsoever in committing crime;
- Larger volume cash deposits/withdrawals and mutual electronic transfers between accounts of natural and legal persons (payment chains aimed at obscuring financial flows).

Methods of UTs may be, in particular:

1. Artificial increase in turnover in the case of firms dealing with cash. Proceeds from crime in the form of cash are mixed with proceeds from legal activity, with the result of the mixing being declared as legal income and legal turnover;
2. Funds transfers from abroad to payment accounts of natural persons or legal persons, followed by their immediate transfer of almost the whole credited amount, or an attempt at cash withdrawal, where there is the risk of frustrating seizure of that income for the purposes of criminal proceedings. This concerns in particular revenues from such activities as phishing, pharming, vishing, internet fraud, payment card fraud, payment terminal fraud;
3. Transfers between companies with an unclear ownership structure that do not have any apparent economic basis or reason;
4. Dealing in arms and hazardous materials that is covered by fake trades or financial operations made by companies domiciled in a tax haven, with local payment accounts being used only for transfer and for obscuring financial flows;
5. Reverse loan, most often using payment accounts of foreign natural or legal persons, usually domiciled in a tax haven;
6. Payments made by non-profit organisations, non-investment funds and foundations, or in their favour, that do not correspond to the purpose of their establishment;
7. Use of payment accounts, in particular those of natural persons, for on-line betting and online gambling;
8. A product, service or transaction in which the customer refuses to provide information on imminent operation, or seeks to provide as little information as possible, or provides only information that the obliged entity can check with great difficulty or at high cost;
9. Repayment of a loan where the whole amount is repaid at once or in several larger instalment payments;
10. Repayment of a customer's loan by an entity which does not have any apparent relation with the customer;
11. A customer conducts trades with entities about which the obliged person has information indicating that they conducted a UT in the past, or with entities which were loosely connected with a completed UT;
12. The financial institution has doubts about the veracity of a customer's identification data it obtained and the customer refuses to be identity checked or to provide identification data of the entity on behalf of which they act;
13. Any financial transactions where a customer, when requested, refuses to provide further information or provides explanation which is hard to believe or difficult to verify;
14. A customer performs activities that may help to conceal their identity or the identity of the real owner;
15. A product, service or transaction in which the volume of funds that the customer uses is in clear disproportion to the nature or scope of the customer's business activity or declared

financial circumstances, or where the customer's payment account movements do not correspond with the nature or scope of the customer's business activity or usual financial transactions;

16. Number of movements on a payment card account, or a higher number of financial transactions conducted in one day or several consecutive days, which goes beyond the ordinary scope of the customer's transactions, while the customer attempts to significantly exceed, for no apparent reason, the financial limit set in the contract with the financial institution;
17. A product, service or transaction made by natural or legal persons associated with an increased risk of money laundering or terrorist financing;
18. A product, service or transaction that, with regard to its complexity, unusually high volume of funds or other characteristic, clearly deviates from the ordinary framework or nature of the product, service or transaction of the particular type or particular customer, or that has no clear economic or lawful purpose;
19. A product, service or transaction in which the customer requests the establishment of a contractual relationship or execution of a financial transaction with the obliged entity on the basis of an unclear project;
20. A product, service or transaction in which the customer submits false, invalid or stolen identification documents, falsified documentation, etc.;
21. Repeated and frequent changes to the right of disposal on the basis of an authorisation granted by the payment account owner;
22. Opening of payment accounts or performance of financial transactions, particularly for foreigners, through an authorised person;
23. Large sums of money transferred to or from abroad using payment services;
24. A product, service or transaction in which there is a reasonable assumption that its subject is or should be a thing or service that may relate to a thing or service on which international sanctions have been imposed under a separate regulation;
25. A product, service or transaction made from or to a country with an increased risk of terrorist financing or a country with a high security risk (drugs, weapons, etc.);
26. High growth in payment account balances that is not in accordance with the customer company's known and normal turnover, and their subsequent transfer to an account (or accounts) abroad;
27. Products, services or transactions involving limited liability companies in which there has been a change in the position of executive, a change of company name, a change of registration court, etc.;
28. Number of movements on a payment account in one day or several consecutive days which goes beyond the ordinary scope of the customer's financial transactions;
29. Customers' activity relating to the opening of multiple payment accounts, the number of which is in clear disproportion to the line of business, and the related transactions between these accounts;
30. Repeated back-transfers of funds to foreign financial institutions and banks domiciled in high-risk areas or to companies domiciled in high-risk areas;
31. Products, services or transactions involving newly-incorporated companies registered in tax havens;
32. Involvement of a firm or financial institution from a high-risk country in a transaction;
33. Customer transferring large sums of money abroad or from abroad clearly at variance with the information available to the financial institution;
34. Internet lottery and gambling, crediting a player's account and subsequent pay-out from the account to a different account without actual gambling or only in a negligible amount;

35. Transfer of funds from the payment account made immediately after the funds were received from a different account;
36. Notice of a change of address, prior to the contract on the opening of an account is delivered by courier, as compared to the address stated when filling in the data in the contract online via the internet;
37. Financial transactions made on a payment account where payments are in low nominal values, though in an extraordinarily high total volume;
38. Repeated fulfilment of a customer's obligations (mainly repayment of their debt) by a third party whose business activities are unknown to the financial institution, whereas the fulfilment involves unusually high amounts;
39. Customer comes from a country in which anti money laundering and counter terrorist financing measures are applied insufficiently or are not applied at all;
40. Where the financial institution allows customers cash deposits and withdrawals:
    - a one-time cash deposit to a payment account that does not correspond to the customer's hitherto activities and information that the financial institution has available on the customer;
    - frequent repetition of cash deposits for no apparent reason, and through the depositing of which a large deposit accrued and was then transferred to a place that, under ordinary circumstances, is not associated with the customer;
    - unusually high cash deposits made by a natural or legal person in business activities in which other instruments would normally be used;
    - a cash deposit to a payment account and subsequent request by the customer to issue a confirmation of the current account balance, followed by a withdrawal from the account;
    - cash deposit or transfer abroad, where the customer states the payment purpose as a fee or commission;
    - repeated cash deposits by a large number of customers who make payments to the same account with no apparent purpose;
    - unusually high deposit of funds to a payment account of a natural person who is a politically exposed person, and which goes beyond the ordinary scope of movements on that account;
    - payment from abroad, particularly a country outside the EU, with its description stated as donation, aid, loan, etc. and its immediate withdrawal in cash or immediate transfer to a different account;
    - cashless credit of a high amount to the customer's account followed by cash withdrawals of lower amounts;
    - a customer has an unusually high volume of cash, which does not correspond with their appearance and behaviour;
    - a customer is accompanied and monitored by another person when concluding a contract or making a cash deposit.