Methodological Guideline
of the Financial Market Supervision Unit of Národná banka Slovenska
No 3/2019 of 29 April 2019
on the prevention of money laundering and terrorist financing
at banks and branches of foreign banks

Národná banka Slovenska, Financial Market Supervision Unit, 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 Criminal Agency of the Presidium of the Police Force of the Slovak Republic, has issued this Methodological Guideline:

PART I

Article 1

Purpose

(1) The purpose of this Methodological Guideline is to provide financial institutions with explanatory material for performing their duties arising from legal regulations concerning the prevention of money laundering and terrorist financing in the financial system, which are based not only on binding Slovak legislation, but also on international standards and, not least, on knowledge, experience and practice gained during the performance of supervision and control by Národná banka Slovenska and the Financial Intelligence Unit of the National Criminal Agency of the Presidium of the Police Force of the Slovak Republic.

(2) Financial institutions shall perform the duties and exercise the rights laid down in Act No 297/2008 on the prevention of money laundering and terrorist financing (and amending certain laws), as amended, whilst proceeding also in accordance with other legal regulations, in particular with Act No 483/2001 on banks (and amending certain laws), as amended, Act No 492/2009 on payment services (and amending certain laws), as amended, Act No 289/2016 on the imposition of international sanctions (and amending Act No 566/2001 on securities and investment services (and amending other laws) – the Securities Act – as amended).

(3) In preparing this Methodological Guideline, the authors have worked from the fact that the rules laid down by the relevant legal regulations represent minimum requirements; the authors, through this Methodological Guideline, neither can, nor seek to, 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 laws and by this Methodological Guideline, financial institutions may also use more sophisticated methods, particularly those already used and proven in their own practice or that of their parent companies from other Member States of the European Union (hereinafter 'the EU') and of the European Economic Area (hereinafter 'the EEA'). In so doing they can better contribute to the implementation of the global AML/CFT policy within the framework of the financial group of which they are part.

(4) Financial institutions are, in the course of their business, exposed to the risk that customers will misuse their services for money laundering or terrorist financing. In the event

of such misuse, the financial institution concerned faces the threat not just of financial loss, but also reputational harm. The main barriers against efforts to misuse a financial institution for money laundering or terrorist financing consist primarily in the integrity and honesty of the management and its commitment to actively enforce the financial institution's policy for the prevention and detection of money laundering and terrorist financing and to promote strict compliance with the legal regulations relevant to these areas.

Article 2

Definition of selected terms

For the purposes of this Methodological Guideline the following terms and abbreviations are used. The definitions of other terms and abbreviations may be stated directly in the text, where appropriate.

Banking Act	Act No 483/2001 on banks (and amending certain laws), as amended.
AML Act	Act No 297/2008 on the prevention of money laundering and terrorist financing (and amending certain laws), as amended.
Payment Services Act	Act No 492/2009 on payment services (and amending certain laws), as amended.
International Sanctions Act	Act No 289/2016 on the imposition of international sanctions (and amending Act No 566/2001 on securities and investment services /the Securities Act/), as amended.
Bank	a legal person established in the Slovak Republic as a joint-stock company operating in the country as a credit institution under Article 2 of the Banking Act
Foreign bank branch	a branch of a foreign bank operating in the Slovak Republic under Article 2(8) of the Banking Act
Financial institution	a bank or a branch of a foreign bank
AML/AML area	area of protection against money laundering and terrorist financing
AML/CFT	anti-money laundering/combating the financing of terrorism
FIU	Financial Intelligence Unit of the National Criminal Agency of the Presidium of the Police Force of the Slovak Republic
NBS	Národná banka Slovenska
UT	unusual transaction
Employee	employee of a financial institution
Money laundering	the legalisation of proceeds from criminal activity
NRA	National Risk Assessment in the AML area

PART II

Article 3

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

(1) Financial institutions should formulate their own policy in respect of the prevention and detection of money laundering and terrorist financing (hereinafter referred to as 'AML/CFT policy'). The AML/CFT policy should be designed so as to ensure effective performance of activities aimed at preventing and detecting money laundering and terrorist financing attempts at the financial institution concerned. Suitable tools and valuable sources of information for planning and implementing a financial institution's AML/CFT policy include Slovak and international standards, the opinions and guidelines of Slovak and foreign regulators, analyses by major Slovak and foreign institutions or consultancy firms, and not least also the experience and approach of other companies within the group of which the financial institution is part.

(2) In creating and applying the AML/CFT policy, the financial institution shall take into account:

(a) its business objectives and business plan;
(b) the composition of its existing clientele, including the number and risk profile of customers;
(c) the range of banking activities, types of transactions, geographical risks, distribution channels through which transactions are carried out and the associated potential threat of their misuse for the purposes of money laundering and terrorist financing.

(3) The AML/CFT policy forms a part of a financial institution's risk management system with special relevance to operational risk management.

(4) The AML/CFT policy consists of the following components:

(a) an organisational structure ensuring the effective and independent performance of AML activities;
(b) the programme of own activity pursuant to Article 20 of the AML Act (hereinafter the 'Programme');
(c) information for customers and the general public, setting out the financial institution's approach and objectives in relation to AML, as well as a notice drawing attention to its duties of prevention and control that may have a direct impact on customers.

(5) A bank's articles of association shall define the bank's organisational structure and system of management, as well as the responsibilities of persons and units in respect of the management of risks to which the bank is exposed in its business.In determining its organisational structure pursuant to subparagraph (4)(a), the bank shall designate a member of the statutory body with responsibility for the area of AML (hereinafter referred to as the 'Responsible Person').

(6) In determining its organisational structure pursuant to subparagraph (4)(a), a foreign bank branch shall designate a senior manager with responsibility for the AML area, or shall designate that the head of the branch is responsible for the AML area (hereinafter the 'branch's Responsible Person').

(7) A bank's AML/CFT policy shall be approved in writing by the bank's statutory body, which is responsible for its implementation. The AML/CFT policy of a foreign bank branch shall be approved by the branch's Responsible Person.

(8) Information and facts as specified in subparagraph (4)(c) shall be published on the website of the financial institution concerned.

Article 4

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

(1) A bank's statutory body is responsible for the bank's overall protection in the AML area and for implementing its AML/CFT policy.

(2) The head of a foreign bank branch is responsible for the branch's overall protection in the AML area and for implementing its AML/CFT policy.

(3) Responsibility for the practical implementation of activities in the area of AML, primarily the performance of day-to-day activities ensuring the implementation of the AML/CFT policy, the reporting of unusual transactions (hereinafter 'UTs') and for ongoing contact with the Financial Intelligence Unit (hereinafter the 'FIU') lies with the Nominated Officer (hereinafter the 'NO').

(4) It is not appropriate to outsource the activities of the NO.

(5) Financial institutions shall ensure full substitutability for the post of the NO, by nominating a deputy NO.

(6) In filling the posts of the NO and deputy NO, financial institutions shall require candidates to prove that they are of good repute and have appropriate education and corresponding professional experience.

(7) The NO and deputy NO of a bank shall be appointed and dismissed by the bank's statutory body, following prior consultation with the supervisory board, or with its chairman. The NO of a bank shall report to the Responsible Person.

(8) The NO of a foreign bank branch shall be appointed and dismissed by the head of the branch. The NO of a foreign bank branch shall report to the Responsible Person.

(9) A financial institution's Programme shall, in accordance with Article 20(2)(h) of the AML Act, contain the full name and position of the NO as referred to in paragraph (3), unless the NO is the statutory body or a member thereof, who shall ensure the performance of AML tasks, the reporting of UTs, and ongoing contact with the FIU. The NO must be a senior manager, must be in direct contact with the statutory body and supervisory board, and must have access to the information and documents that obliged persons have obtained while exercising customer due diligence.

(10) Under Article 7(21) and Article 9(4) of the Banking Act, a senior manager is a person directly reporting to the statutory body of a bank or to the head or deputy head of a foreign bank branch and managing the activities or part of the activities of the bank or foreign bank branch concerned. The appointment of a senior manager requires prior approval from Národná banka Slovenska, otherwise the appointment is considered invalid. Under Article 23(1), (2) and (5) of the Banking Act, banks are required to establish in their articles or

association and internal regulations a detailed organisational structure and to define the relationships and forms of cooperation between their statutory body, supervisory board, senior managers, internal control and internal audit unit, and to ensure that the said structure complies with the requirements laid down by the Banking Act.

(11) An important element of AML/CFT policy is to ensure that the NO and their deputy have a sufficiently independent status in the structure of senior managers and organisational units. The NO's classification in a financial institution's organisational structure shall include the following elements guaranteeing an appropriately defined standing for the NO and their deputy:

(a) arrangement of powers and duties of the NO and their deputy in their job descriptions, with emphasis on the primary area of their operation, which is to ensure the prevention of money laundering and terrorist financing;
(b) separation from units responsible for carrying out transactions and financial operations for customers;
(c) unlimited access of the NO and their deputy to all documents, databases and information at the financial institution;
(d) autonomous and independent decision-making by the NO and their deputy in assessing the suspiciousness of customers' transactions reported by the respective staff within the framework of the internal reporting system;
(e) autonomous and independent decision-making on the sending of UT reports to the FIU;
(f) a control function of the NO and their deputy in relation to the units and employees responsible for conducting transactions and financial operations for customers;
(g) separation of the NO and their deputy from the internal control and internal audit unit in the organisational structure, whilst preserving follow-up inspection of their activity conducted from the side of the internal control and internal audit unit;
(h) cooperation with the internal control and internal audit unit in the procedure outlined in Article 41(2) of the Banking Act, and the powers to participate in the process of commenting on and/or evaluating new types of transactions and new transaction processing methods that are under preparation at the financial institution in terms of the risks inherent in money laundering and terrorist financing, and to express a dissenting opinion on such transactions;
(i) in the case of extraordinarily serious circumstances or situations related to an NO's activities, immediate notification of a member of the statutory body, in the case of a bank, or the Responsible Person, in the case of a branch.

(12) The job description of a financial institution's NO shall include in particular:

(a) preparation and continuous updating of the financial institution's Programme and any other necessary regulations and procedures for the AML area;
(b) performance of management and control tasks in the area of AML;
(c) communication and cooperation with the FIU, including timely reporting of UTs;
(d) communication and cooperation with NBS;
(e) organisation and setting of rules for training the financial institution's staff, including new staff;
(f) analytical and advisory activities in relation to the assessment and reporting of UTs by the respective staff in connection with the conduct of transactions and financial operations for customers.

(13) A bank's NO and their deputy shall perform their tasks with due professional diligence. The NO shall submit a report on their AML activities to the bank's statutory body at least once a year.

(14) The NO of a foreign bank branch shall submit a report on their AML activities to the Responsible Person and head of the branch at least once a year.

(15) An activity report shall contain in particular the following information:

(a) statistics and a brief description of UTs reported by the financial institution's staff;
(b) statistics and a brief description of UTs reported to the FIU;
(c) statistics and a brief description of unreported UTs;
(d) statistics and a brief description of UTs that were not reported to the FIU, with reasoning;
(e) an overview of identified deficiencies and draft measures and deadlines for their rectification;
(f) information obtained from inspections carried out;
(g) information on, or an overview of, staff training conducted.

(16) Before an employee enters employment at a financial institution in a post or function where they will, in direct contact with customers, ensure the execution of payment operations, the financial institution shall, on the basis of a criminal record check certificate issued to the potential employee, ascertain that the potential employee has not been lawfully sentenced for any property-related, economic or other serious criminal offence. This procedure also applies to the financial institution's existing staff, including senior managers in charge of assessing transactions pursuant to Article 14 of the AML Act.

(17) In addition to the criminal record check certificate under paragraph (16), a financial institution may require from a potential employee the following additional information:

(a) information beyond the framework of a criminal record check certificate (but in so doing, it should take account of the fact that, under Article 93 of Act No 300/2005 – the Criminal Code, as amended, if the conviction of a person has been expunged, this person is to be viewed as if they had not been convicted);
(b) a sufficiently satisfactory reference, or assessment of the potential employee's prior work integrity, issued by their previous employer; or
(c) other information.

(18) For a more objective assessment of a potential employee's good repute, the financial institution may require other supporting documents and information related to their good repute.

Article 5

A financial institution's programme of own activity

(1) Financial institutions are required to draw up an activity programme in accordance with Article 20 of the AML Act, which shall be approved by the statutory body of the bank or head of the foreign bank branch concerned. The Programme shall be based on generally binding legal regulations, in particular the AML Act, the Banking Act, other relevant laws, the methodological guidelines of the FIU published and regularly updated on the FIU's website (http://www.minv.sk/?Metodicke-usmernenia-a-stanoviska-FSJ), and on FATF Recommendations and EU legislation pertaining to AML.

(2) A financial institution's Programme must reflect its specific characteristics, in particular:

(a) its size and market share, organisational structure, number of employees, method of management, the type and range of permitted banking activities, the types of transactions, the type and number of customers, and the most frequent forms of UTs;
(b) the financial institution's articles of association and AML/CFT policy;
(c) the powers, duties, responsibilities and tasks of the financial institution's NO and those of its internal control and internal audit unit;
(d) information flows, information systems, control processes and mechanisms in this field;
(e) operational procedures and duties of the financial institution's staff in executing the relevant types of transactions and payment operations for customers;
(f) assessment, evaluation and updating of money laundering risks, including NRA results pursuant to Article 26a of the AML Act.

(3) The Programme shall set out in particular:

(a) an overview of known types of UTs, broken down by activity and type of transaction executed;

(b) the detailed signs of unusualness by which the UTs of customers can be recognised;

(c) the manner in which customer due diligence is performed;

(d) the determination of the manner and scope of customer due diligence performance based on the results of a risk assessment pursuant to Article 10(4) of the AML Act;

(e) the assessment and management of risks associated with money laundering and terrorist financing, 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 transaction, payment operation and account and by the customer's risk category;

(f) the selection of persons within the financial institution who shall assess whether an imminent or ongoing transaction is unusual;

(g) the setting of the time when such assessment is to be carried out (where possible, always before the execution of a transaction or in the process of its preparation);

(h) the method and process of risk assessment pursuant to points (f) and (g), including the tools to be used in assessing the risks and recording the assessment results, i.e. to state what needs to be done during such assessment, what aids are to be used (e.g. an overview of the forms of UTs, publicly available information on debtors and defaulters, internal lists of customers, etc.), how and where to record the assessment results;

(i) the manner and scope of feedback at the financial institution on internal notifications of UTs (e.g. the Nominated Officers should have an overview and/or feedback on reported UTs, which UTs were reported to the FIU, etc.);

(j) the duty to maintain confidentiality in respect of an internal notification of a UT and its reporting to the FIU and in respect of measures employed by the FIU pursuant to Article 18 of the AML Act, primarily in relation to the customer concerned, as well as towards persons having a certain relationship with the customer (e.g. other authorised users of the customer's account, or where this concerns multiple owners of funds on one account or owners of a legal person or other final beneficiaries associated with the operation), as well

as towards third parties, other than exceptions as provided for by the Act;

(k) arrangements ensuring protection in the area of AML, the receipt of notifications on identified UTs from organisational units, the evaluation of these notifications and the reporting of UTs to the FIU and arrangements ensuring ongoing working contact with the FIU, or with law enforcement bodies;

(l) the specification of the tasks, duties and responsibilities for the comprehensive protection of the financial institution in the AML area at the individual levels of management from the board of directors of the financial institution, or from the Responsible Person of the foreign bank branch, down to the frontline customer-facing units, including the internal control and internal audit unit in charge of AML/CFT tasks;

(m) the definition of information flows and the description of information systems for the collection, processing and reporting of information on AML/CFT, including regular reports submitted to the board of directors and supervisory board of the financial institution and to the Responsible Person or head of the foreign bank branch concerned;

(n) the duty to identify customers and to verify their identification;

(o) the duty to record the identification of customers and verification of their identification;

(p) the duty to archive the records of customer identification and of the verification of their identification, and this for the period set by the Act;

(q) the method and periods of archiving for data and documentation;

(r) the identification of the NO pursuant to Article 20(2)(h) of the AML Act;

(s) the procedure used by the respective staff and NO to delay a UT pursuant to Article 16 of the AML Act;

(t) the specification of basic tasks of the relevant staff at all levels of management, the detection of UTs and the reporting of internal notifications of UTs to the NO, including the manner of ensuring protection for the respective staff in connection with the UTs they identified and reported to the NO;

(u) the content, timetable and plan of staff training, the training of the financial institution's relevant staff for performing AML/CFT tasks while conducting specific banking activities, transactions and operations for customers;

(v) measures and control mechanisms preventing the abuse of position or function by members of the relevant staff to knowingly engage in money laundering or terrorist financing during the performance of their function;

(w) an internal control system focused on AML/CFT, consisting of control mechanisms, process controls of senior managers, including controls by the NO and internal auditors;

(x) the schedule and method of staff training and information in accordance with Article 6(4).

(4) The AML/CFT issue requires that the Programme be drawn up as an integral regulation accessible to all members of the financial institution's staff via an internal computer network or in another form (Article 20(3) of the AML Act).

(5) It is necessary to update the Programme at least once a year. The Programme needs to be updated not only in the event of a change in the relevant legislation of general application, but also in the event of changes concerning the financial institution's own activities and transaction types, before the introduction of new innovative technologies and software products

for the provision of products and services, as well as in the event of changes in the financial institution's organisational arrangements.

Article 6

Staff awareness and training

(1) All members of a financial institution's staff must be aware that a customer's involvement in money laundering or terrorist financing represents an operational risk regardless of whether it is deliberate or the result of unwitting negligence. The financial institution can ultimately suffer financial losses if it executes operations with proceeds from any criminal activity, whilst its reputation may also suffer. Not only financial institutions as legal entities 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 bank branch, the Responsible Person of a branch, senior managers performing control tasks and the respective staff in direct contact with the customer and who execute the customer's instructions for conducting transactions and financial operations may also be held liable.

(2) Success in applying an ongoing AML/CFT process depends on the effective training of staff and their proper familiarisation with their duties and powers. The statutory body of a bank or the Responsible Person of a foreign bank branch, jointly with the NO, must ensure that the staff are aware of both the financial institution's responsibility and their own personal liability and protection as regards the identification of UTs in this area.

(3) Financial institutions shall publish in an appropriate manner information for their staff on who performs the function of the NO and who deputises for the NO.

(4) Financial institutions shall determine in their Programme an appropriate schedule and method for:

(a) informing their staff about the AML/CFT system, the procedures to be followed, and about their duties and powers;
(b) making the Programme and other relevant internal regulations available to the staff;
(c) organising regular staff training and educational activities for the staff; where regular training is performed via e-learning, it is recommended to appropriately supplement e-learning training by personal or other training (e.g. team training) so that the training system is effective.

(5) Financial institutions, in informing and training their staff, shall take account of their conditions, in particular their size and organisational arrangement (branches, or other smaller workplaces), banking activities, and types of transactions and financial operations performed for customers, so that all the necessary information reaches the staff for whom the information is intended. It is important that the mechanism of providing information to the staff from the side of the statutory body, the Responsible Person in the case of a foreign bank branch, the NO and respective senior managers of the financial institution concerned, 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 in response to changing conditions.

(6) Front office staff must have all the necessary information on the banking activities and types of transactions they execute for customers and they must learn as soon as possible the criteria for assessing, or detecting, UTs.

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 unusualness and the degree of risk involved. Staff training should significantly contribute to employees' acquisition of the prerequisites for mastering procedures for applying the 'Know Your Customer' principle (hereinafter referred to as 'KYC') and for recognising the degree of risk involved in 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 customer due diligence.

(7) In providing training, financial institutions shall ensure that their staff are familiarised with the consequences of negligence or negligent performance of their work duties and of any knowing or unwitting participation in money laundering or terrorist financing, and with the consequences of a breach of the prohibition of providing customers with information to which a duty of confidentiality applies (Article 18 of the AML Act), as well as with the manner of their protection if they detect a UT.

(8) Financial institutions must have a plan of staff training drawn up in respect of the work classification of their employees (own categorisation according to job positions, taking into account the exposure of employees 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 plan of training, 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 competent employee must be familiarised with the applicable Programme governing the procedures to be followed in assessing customers and their payment operations. At the same time, the financial institution is required to ensure that each employee has permanent access to the Programme in the manner set out in Article 5(5).

(10) Staff training (education) shall include in particular:

(a) familiarisation with the Programme;
(b) familiarisation with the AML Act;
(c) familiarisation with EU legislation;
(d) knowledge and experience gained from the activities of:
    1. nominated officers;
    2. other financial institutions (e.g. knowledge about the AML practices of other financial institutions, which can be used in staff training);
    3. the FIU and NBS;
    4. domestic or international financial institutions in the area of AML (e.g. knowledge about the activities of domestic or international financial institutions, including knowledge about the AML practices of the financial group to which the financial institution belongs, which can be used in staff training);
(e) practical examples from AML/CFT, including information, findings and shortcomings if any, acquired by financial institutions during their internal control activities;
(f) induction courses for new employees;
(g) specialised training courses;

(h) familiarisation with the results of staff training completed in accordance with paragraph (15).

(11) The induction course that a financial institution's staff must complete before they process customers' instructions for the execution of payment operations is supposed to give them the necessary knowledge for ascertaining and verifying a customer's identity when establishing a business relationship and executing a transaction or payment operation.

(12) In determining the frequency of training, financial institutions shall observe the provisions of Article 20(3) of the AML Act (at least once per calendar year and always before an employee is assigned to work).

Financial institutions should repeat and supplement training (education) with new knowledge, where necessary, also more frequently than in a 12-month cycle, so as to ensure that the relevant staff are able to continuously perform their duties and exercise their powers.

(13) Financial institutions should, in the framework of staff training, apply and regularly update the following forms of training:

(a) classic training (lecturers);
(b) electronic training (e-learning, tests, individual study of laws, etc.);
(c) job rotation;
(d) coaching and mentoring;
(e) random testing of the staff at the workplace;
(f) combined forms of training as listed under points (a) to (f);
(g) other forms of training.

(14) Financial institutions shall, in the framework of staff training, ensure that their employees receive feedback on any training they have completed. In verifying the effectiveness of staff training, financial institutions should use a limited number of repetitions (it is ineffective to verify the result of training by way of multiple testing with an unlimited number of repetitions).

(15) Financial institutions shall draw up records of the staff training events they organise, containing the date, content and form of training, and, where relevant, an evaluation of the tests completed, as well as the employees' signatures or other electronic confirmation.

(16) Through participation in training events, a financial institution's staff will acquire the necessary knowledge and capability to identify facts outside the expected behaviour of customers, and specific manifestations of their UTs. The frequency of staff training should be set so that the risks of money laundering and terrorist financing are fully covered at all times.

Article 7

Information system at a financial institution

(1) A systemic approach to a financial institution's risk management and AML/CFT systems 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 systemic approach for ensuring information flows also requires support in the form of application software, i.e. a specialised information system, or systems.

(2) In broad terms, the information system mentioned in paragraph (1) means a system for acquiring, processing, evaluating, transferring and also using information concerning this area. The system includes flows of AML/CFT information in the processes of the financial institution's individual activities and types of transactions performed.

(3) For effective money laundering prevention, it is essential to ensure that the information system is regularly updated, with an emphasis on the timely introduction of new types of transactions and procedures in that system.

(4) In addition to information systems and application software for ensuring information flows for the AML/CFT system, the financial institution may use a specialised automated system to support the detection of UTs and persons subject to sanctions in the financial institution's relevant information systems; that system will operate on the basis of set scenarios in databases of customers, transactions or payment operations.

(5) Financial institutions are 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) the transmission of necessary information between the statutory body, senior manager or head of a foreign bank branch, and the NO;
(d) the transmission of information between the staff and the NO and vice versa, including internal notifications of UTs;
(e) record-keeping, i.e. the recording, processing and updating of data on customers and the recording and monitoring of customers' transactions;
(f) notifying the statutory body or Responsible Person of the results of control performed by the NO and the internal control and internal audit unit, as well as informing the staff of these results;
(g) the transfer of information between the NO and FIU, including UTs, and the 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;
(h) searching for UTs in the financial institution's relevant information systems that contain data on customers and their transactions.

(6) In ensuring information flows pursuant to subparagraph (5)(e), financial institutions should also take into account types of transactions and their respective risks in the AML area. In the case of higher-risk transactions, financial institutions should consider specific measures appropriate to the risks involved in the transaction.

(7) Specific measures for selected types of risky transactions should be set by a financial institution separately for each transaction that is identified as a higher-risk transaction in the area of AML. In setting specific measures, the financial institution should consider primarily the risk factors listed in Annex 1 (mainly in Parts 2, 4 and 5).

(8) A financial institution should set the form, content and rules of information flows having regard for its size, focus, the range and complexity of its activities, the types of transactions and services offered, and the characteristic features of its customers and their transactions.

(9) The components of a financial institution's information system as referred to in paragraph (1) include an electronic information system (hereinafter referred to as an 'EIS') that complies with the requirements laid down in Article 7(1) of the AML Act, designed to record and manage data on customers and on their payment transactions:

(a) in the case of a natural-person customer, the EIS must contain the customer's full name, birth registration number if assigned or date of birth, address of permanent residence or other residence, citizenship, identification document (type and number), and the customer's account number;
(b) in the case of a natural-person entrepreneur, the EIS must contain the same data as under point (a), plus place of business address, identification number if assigned, designation of the official register or other official record in which the natural-person entrepreneur is registered, and the number of his entry in this register or record;
(c) in the case of a legal-person customer, the EIS must contain at least the customer's trade name, registered office address, identification number, the designation of the official register or other official record in which the legal person is registered, the number its entry in this register or record, and data on the natural person authorised to act on behalf of the legal person, as under point (a).

(10) In addition to the data specified in paragraph (9), the EIS must contain information or records on the purpose and nature of the customer's business relationship. The nature of a business relationship is given by the type of transactions as per Article 9(h) or solely by a transaction as per Article 9(g), whilst the nature of the business relationship is primarily predetermined by the actual product or service that the customer uses. The EIS and the manner of using it should make it possible to identify UTs made by customers, and, as relevant, monitor also their course or development, as well as the connections between the transactions of a certain customer and, where possible, also the unusual transactions of different customers.

(11) A special part of the information recorded and monitored by the EIS consists in data on:

(a) politically exposed persons as referred to in Article 6 of the AML Act;
(b) the beneficial owner as referred to in Article 6a of the AML Act; and
(c) shell banks as referred to in Article 9(c) and Article 24(l) of the AML Act, which the respective staff detected in performing their work tasks.

(12) The EIS must enable the financial institution to respond promptly to a request from the FIU with information as to whether it has d a business relationship with a specified person or has had such a relationship in the past five years, as well as on the nature of that business relationship pursuant to Article 21(1) of the AML Act.

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

Article 8

Customer identification and customer acceptance, customer risk profile; basic, simplified and enhanced customer due diligence

(1) In identifying a customer and verifying the customer's identification, financial institutions shall proceed in accordance with Articles 7 and 8 of the AML Act. As part of this process, financial institutions shall also verify whether the customer is on the list of persons subject to sanctions.

(2) Financial institutions shall apply all elements of basic customer due diligence in accordance with Article 10(1) of the AML Act, always in situations mentioned in paragraph (2) of the AML Act.

(3) Where basic customer due diligence cannot be applied under Article 10(1)(a) to (e) of the AML Act, financial institutions shall refuse to enter into a business relationship, terminate an existing business relationship, or refuse to execute a specific transaction in accordance with Article 15 of the AML Act.

(4) Under Article 17(1) of the AML Act, financial institutions shall report the cases mentioned in paragraph (3) to the FIU.

(5) In the case of a one-off transaction outside a business relationship, financial institutions shall identify the customer and verify the customer's identification pursuant to Article 10(3) of the AML Act, in all cases where the transaction value is at least €1,000. Depending on the degree of risk assessed pursuant to Article 20a of the AML Act, financial institutions may set the threshold to a lower transaction value where there is a higher risk of money laundering and terrorist financing.

(6) Financial institutions shall ascertain whether a customer is acting on their own behalf pursuant to Article 10(7) of the AML Act in situations mentioned in Article 10(2) of the same Act and in accordance with Article 89(4) of the Banking Act, even where this concerns a transaction amounting to at least €15,000, or €10,000 in cash.

(7) Financial institutions shall identity the beneficial owner and verify their identification in accordance with Articles 6a, 7, 8 and 10 and the AML Act.

(8) 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 an asset association, 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 property association, a natural person who:
1. is the founder of the property association, or, if the founder is a legal person, a natural person as referred to in subparagraph (a);
2. has the right to appoint, otherwise establish, or dismiss the property association'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 property association'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 property association, 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 property association's establishment or operation.

(9) Under Article 6a of the AML Act, the beneficial owner should be identified by the financial institution always where it is:

(a) a legal person as referred to in Article 6a(1)(a) of the AML Act;
(b) a natural-person entrepreneur as referred to in Article 6a(1)(b) of the AML Act;
(c) a property association as referred to in Article 6a(1)(c) of the AML Act.

(10) Where no natural person meets the criteria laid down in Article 6a(1) of the AML Act, the beneficial owner will be a member of the top management, which may be:

(a) the statutory body;
(b) a member of the statutory body;
(c) the authorised representative;
(d) a senior manager reporting directly to the statutory body.

(11) In identifying the beneficial owner, a financial institution shall record the following data:

(a) in the case of a legal person as per subparagraph (9)(a), the name, registered office address and identification number of the legal person, the designation of the official register or other official record in which the legal person is registered, the number of its entry in this register or record, and data on the natural person authorised to act on behalf of the legal person concerned;
(b) in the case of natural-person entrepreneur as per subparagraph (9)(b), the full name, birth registration number if assigned or date of birth, address of permanent residence or other residence, citizenship, identification document (type and number), place of business address, identification number if assigned, the designation of the official register or other official record in which that person is registered, and the number of entry in this register or record;

(c) in the case of a property association as per subparagraph (9)(c), the data as listed in subparagraphs (a) and (b), depending on whether the beneficial owner is a natural person or a legal person.

(12) The identification of a beneficial owner and the adoption of appropriate measures for verifying the beneficial owner's identification shall be ensured by the financial institution concerned, in accordance with the provisions of Articles 7(1)(a) and 10(1)(b) of the AML Act.

(13) The verification of a beneficial owner's identification may be completed during the establishment of a business relationship where the conditions set out in Article 8(3) and (4) of the AML Act are met.

(14) An obliged person as referred to in Article 10(1)(b) of the AML Act shall identify the beneficial owner and adopt appropriate measures for verifying the beneficial owner's identification, including measures for determining the ownership and management structures of the customer if the customer is a legal person or a property association. In identifying the beneficial owner, the obliged person may not rely exclusively on data obtained from a register of legal persons, entrepreneurs and public authorities. If any reasonable doubt arises about the correctness or completeness of the data obtained about the beneficial owner, the financial institution shall again apply basic customer due diligence pursuant to Article 10(2)(d) of the AML Act. If the financial institution cannot identify the beneficial owner, nor adopt appropriate measures for verifying the beneficial owner's identity, including measures for determining the customer's ownership and management structures, it shall refuse to enter into a business relationship, terminate an existing business relationship or refuse to carry out a specific transaction.

(15) Under Article 10(1)(d) of the AML Act, the financial institution must find out whether the beneficial owner is a politically exposed person or a person included on the list of sanctioned persons.

(16) Under Article 93(a) of the Banking Act, the beneficial owner is to be identified always where it is a legal person, though its legal form has no influence on its verification.

(17) In identifying the risks posed by a beneficial owner, the financial institution should take into account in particular the information on risk factors from Annex 1 (mainly from Part 2.1.1 of Annex 1).

(18) In the case of a new customer, the customer acceptance process shall include basic customer due diligence and the categorisation of the customer in a defined risk category to allow the creation of a risk profile for the customer.

(19) In categorising customers into risk groups set up by the Programme, financial institutions shall consider the information on risk factors from Annex 1 (mainly from Part 2 of Annex 1).

(20) Financial institutions shall regularly update the risk profiles of their customers according to the risk categories to which the customers are assigned. The dates of updating of customers' risk profiles according to their categorisation shall be incorporated into the Programme.

(21) By categorising their customers according to their risk profiles, financial institutions can then in practice apply Article 10(1)(g) of the AML Act, namely ongoing monitoring of the business relationship for the detection and reporting of UTs.

(22) Financial institutions may perform simplified customer due diligence in the scope and under the conditions set out in Article 11 of the AML Act. They may use this option, after carefully considering the use of a risk-based procedure, in the case of such situations and customers where it is possible to obtain and verify basic information from publicly available and reliable sources and this information justifies the application of simplified customer due diligence. Before deciding to use simplified customer due diligence, financial institutions shall also consider the option to apply the procedure described in Annex 1 (mainly in Part 3, Chapter 3.1, Annex 1).

(23) The use of simplified customer due diligence in no way represents an exemption from the duty to monitor the business relationship on a continuous basis pursuant to Article 10(1)(g) of the AML Act, or from other duties defined in Articles 14, 17, 19 and 21 of the AML Act.

(24) Financial institutions may apply the elements of enhanced customer due diligence in the scope and under the conditions set out in Article 12 of the AML Act, in order to moderate the degree of risk to an acceptable level. Before deciding to perform enhanced customer due diligence, financial institutions shall also consider the option to apply the procedure described in Annex 1 (mainly in Part 3, Chapter 3.1, Annex 1).

(25) Enhanced customer due diligence is used mainly in the case of:

(a) transactions representing a higher risk owing to their nature;
(b) special categories of customers.

(26) The identification of a natural-person customer who is not physically present using technical means and procedures pursuant to the AML Act, without applying enhanced customer due diligence in the scope specified in Article 12(2)(a) of the AML Act, is described in detail in the Financial Market Supervision Unit's Standpoint No 1/2018 of 10 December 2018, available on the NBS website: (http://www.nbs.sk/_img/Documents/_Legislativa/_Vestnik/Stanovisko1_2018.pdf). During verification, financial institutions shall demonstrate that the scope of customer due diligence is adequate in respect of the risk of money laundering or terrorist financing.

(27) The conditions for the proper application of the KYC principle are derived from the duties of financial institutions and customers, as set out in Articles 10 to 12 of the AML Act. The crucial provisions are those of Article 10(1), (4) and (5) and Article 11(3) of the AML Act. The procedure described in Articles 10(1) and 11(3) of the AML Act enables a financial institution to satisfy itself as to the actual identity of each customer and to identify the purpose and planned nature of commercial 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, and then determining the degree of customer due diligence pursuant to Article 10(4) of the AML Act and for accepting a customer. The 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 the AML Act.

Article 9

Detection, reporting and delay of unusual transactions

(1) Financial institutions are required to assess every imminent or ongoing transaction as to whether it is unusual. Under Article 20(1) and (2)(d) of the AML Act, this part of the procedures must be regulated in every financial institution's Programme. Duties referred to in Article 14(1) and (2)(a) and (b) of the AML Act must be demonstrably fulfilled so that financial institutions can, in accordance with Article 30(3) of the AML Act, in the case of an inspection, provide information and written documents on the fulfilment of these duties.

(2) Under Article 4 of the AML Act, an unusual transaction (UT) 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 AML Act gives a non-exhaustive typology of UTs. For each UT listed in this provision, there are several indicators of unusualness (e.g. an unusually high volume of funds with regard to the type of transaction, an unusually high volume of funds without clear economic or legal purpose, etc.) that financial institutions are required to assess. Only by such action can they competently assess whether a customer's imminent or ongoing transaction is or is not unusual. Article 4 of the AML Act does not stipulate any criteria – e.g. in the form of threshold amounts of funds – that would lead to an automatic finding that a certain type of financial operation undoubtedly constituted a UT.

The decisive element for assessing a customer's transactions is the application of the KYC principle and the proper recognition of indicators of unusualness, as well as other signs or criteria that financial institutions are required to determine for themselves, depending on the subject and scope of their activities and the type and extent of transactions and financial operations performed for customers in the framework of drawing up an overview of the forms of UTs (Article 20(2)(a) of the AML Act).

(3) Financial institutions are required, in applying each type of customer due diligence, to assess whether an imminent or ongoing transaction is unusual (Article 14(1) of the AML Act) 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 of them in accordance with Article 14(3) of the AML Act (i.e. internal reporting of UTs, system analysis, etc.). The record of assessment must include information justifying the result of assessment. Financial institutions are required to archive these records for the period referred to in Article 19 of the AML Act.

(4) Financial institutions shall carry out a skilled assessment of imminent and ongoing transactions pursuant to Article 14 of the AML Act at various time intervals and at various levels. The assessment process takes place:

(a) on the front office, 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 follow-up (retrospective) assessment of a customer's transactions.

(a) assessment of transactions in front office contact with customers before and during the execution of a transaction

The assessment of a customer's transactions is carried out by the financial institution's staff who, in fulfilling their duties, are in contact with the customer, particularly those staff

members who receive or process a customer's instructions for executing the customer's transactions or financial operations. This means in particular front office staff, cashiers, staff arranging the execution of money transfers or payments and other staff involved in the provision of services to customers and processing of data. The assessment of a transaction by an employee of the financial institution is, thus, performed largely at the place where the transaction is executed and prior to its execution, or at an attempt to execute a transaction so that a UT can be delayed and promptly reported to the FIU.

Another crucial element for assessing a customer's transactions here is the proper application of the KYC principle and its procedures and the skilled identification of signs of unusualness. This procedure enables the employee to assess a customer's imminent or ongoing transactions by comparing them against an overview of forms of UTs (Article 20(2)(a) of the AML Act), as well as against forms referred to in Article 4(2) of the AML Act and to detect those that are unusual in relation to the customer and their otherwise usual transactions. If an employee judges an imminent or ongoing transaction to be unusual, they shall make a written record of this transaction in accordance with Article 14(3) of the AML Act and promptly report this finding (send an internal notification of the UT) to the Nominated Officer.

(b) assessment of transactions in the framework of ongoing monitoring of a business relationship

Depending on whether assessment applies to:

1. an existing business relationship (Article 10(2)(a) of the AML Act), or
2. an occasional transaction outside any business relationship (Article 10(2)(b) of the AML Act), the relevant staff of the financial institution shall assess the customer's transactions also in the framework of ongoing monitoring of the relevant business relationship.

The assessment of imminent or ongoing transactions in the framework of ongoing monitoring of the business relationship is specific in that the business relationship has already arisen and continues. The customer may also be known to the financial institution where the customer has already executed several occasional transactions. This, therefore, is not the first contact with the customer and the financial institution may take account of the customer's existing risk profile and the history of transactions performed by the customer. The procedure according to Article 10(1)(g) of the AML Act, including verification of the completeness and validity of identification data and information under Article 10(6) of the AML Act and the customer's duty under Article 10(5) of the AML Act form the basis for the 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 the AML Act.

Ongoing monitoring of a 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 some of the signs of unusualness of customers' transactions so as to allow their differentiation into certain levels of the monitoring process, corresponding to the degree of risk inherent in the operations performed by customers. The set criteria or limits defined by the financial 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 transactions, importance shall be given, in the framework of ongoing monitoring of the business relationship, to imminent or

ongoing transactions of a customer that do not correspond to the customer's known or expected activity. Such transactions of a customer shall form the subject of assessment and it is necessary to make a written record of them, which must also contain information justifying the result of assessment.

The NO may, based on their assessment of the various circumstances of a transaction, conclude that in the given case it does not constitute a UT. If this cannot be done using only the information on the customer that the financial institution already has available, it may, according to the circumstances, request other necessary information and documents from the customer, pursuant to Article 10(5) of the AML Act. In the cases where the NO is unable, even through this procedure, to identify the reason for the customer's transactions, it is sufficient that these operations merely indicate the fact that their execution may constitute money laundering or terrorist financing, and the NO is required to report the UT to the FIU.

Other staff and the NO may participate in the assessment of transactions in the framework of ongoing monitoring of the business relationship depending on the transaction concerned.

(c) assessment of transactions in the framework of follow-up or retrospective assessment of a customer's transactions

A means of follow-up monitoring of customers' transactions is, for example ex-post random selection of executed transactions in the framework of an inspection from the side of a senior manager superior to the employee who executed the customer's instructions and operations, as well as in the framework of an inspection performed by the NO and internal control unit (see part I).

(5) Recommended procedure in the assessment and processing of internal notifications of UTs and UT reports:

(a) all internal notifications of UTs sent by competent staff members to the NO must be documented in accordance with Article 14(3) and must be available for inspection under Article 29 of the AML Act; the written record must contain information justifying the assessment results;
(b) the sending of internal notifications and reports to the Nominated Officer must not be subject to the prior consent of any person;
(c) the NO shall register and archive records of internal notifications of UTs, including the customer's full name and position, the designation of the financial institution's relevant unit, and all data on the given customer and transaction in accordance with Article 19 of the AML Act;
(d) the NO, as well as the staff of the financial institution, including its senior managers involved in the assessment of transactions under Article 14 of the AML Act are required to maintain confidentiality on reported UTs and on measures taken by the FIU (Article 18 of the AML Act), including the fulfilment of duties under the provisions of Articles 17(5) and 21(1) of the AML Act; the financial institution may not, however, cite towards Národná banka Slovenska and the Ministry of Finance of the Slovak Republic the duty to maintain confidentiality in connection with the performance of supervision and inspection under Article 29 of the AML Act (Article 18(5) of the AML Act). Provided that information given is used exclusively for the purposes of preventing money laundering or terrorist financing, the duty of confidentiality shall 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 the AML Act;

(e) the financial institution shall draw up a procedure covering the period from the moment a UT is detected to its prompt reporting, including the procedure and responsibility of the staff who assess the transaction;

(f) the NO, after receiving an internal notification of a UT, may confirm receipt of that notification to the competent staff member who sent that notification. The confirmation should contain an instruction on the duty to maintain confidentiality under Article 18 of the AML Act. Where the financial institution has an electronic system for gathering internal reports that enables the competent staff member to monitor the status or receipt of a submitted internal notification of a UT by the Nominated Officer, no individual confirmation of receipt of such a notification is needed.

(g) internal notifications of UTs, or the conduct of customers, the transactions or financial operations that a notification concerns shall be subject to assessment by the NO, who may, on the basis of results from further assessment of the various circumstances of the transactions, decide whether they do or do not constitute UTs. If a decision cannot be made using only the information on a customer that the financial institution already has available, it may, according to the circumstances, request other necessary information and documents from the customer, pursuant to Article 10(5) of the AML Act. Where the NO reaches the justified conclusion that an internally notified UT does not actually constitute a UT, the NO is required to document this decision in writing and to archive all related data, written and electronic documentation for the period referred to in Article 19 of the AML Act.

(h) in cases where the NO cannot, even through the given procedure, reach the conclusion that it is not a UT, it is sufficient that the transaction or financial operation indicates that its execution may constitute money laundering or terrorist financing, and the NO is required to report the UT to the FIU. A UT or attempt at executing a UT must be reported to the FIU without undue delay. It is constantly necessary to take into consideration the specific circumstances of the situation in which the UT was detected, although a financial institution is required to report a UT as soon as possible. Each report on a UT must have a reference number assigned as a serial number/calendar year. A UT may be reported in writing, electronically or by telephone (in which case it is necessary to report the UT also in person, in writing or by e-mail within three days). The specimen form for reporting a UT, issued by the FIU, is available on the FIU's website (https://www.minv.sk/?vzory-hlaseni-o-noo). In connection with the reporting of UTs, the sending of supplementary information, and the exchange of information and overall communication with the FIU, it is recommended in the interest of compatibility and streamlining of the procedures used in the reporting process, as well as in the interest of streamlining of the control processes, that financial institutions communicate with the FIU by electronic means, while complying with the conditions for protection of the transmitted data and clear identification and verification.

(i) a financial institution may, under Article 92(7)(a) of the Banking Act, keep a register of customers who meet properly and in due time their duties arising from contracts concluded with the financial institution, customers whose conduct has been assessed as constituting a UT, customers about whom the FIU requests information in connection the verification of UTs, and customers subject to international sanctions, and may, under Article 92(7)(b) of the Banking Act, provide information from this register to other financial institutions without the customers' consent; the information provided shall be subject to bank secrecy requirements;

(j) Article 18(8)(a) of the AML Act allows financial institutions, under defined conditions, to exchange information where this is reasonable and relevant to the threat of money laundering or terrorist financing, and where it helps obliged entities to more effectively

assess a customer's 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 UT as a whole, but only specific information relating to the risk of money laundering or terrorist financing. The information provided must, pursuant to the AML Act, be used exclusively for the purposes of preventing money laundering or terrorist financing.

(6) Procedures recommended for delaying a UT:

(a) according to Article 16 of the AML Act, a financial institution shall delay a UT, i.e. a particular transaction (as per Article 9(g)) of the AML Act) that would otherwise be executed;
(b) a financial institution shall, under Article 16(1) of the AML Act, delay a UT until the time of its reporting to the FIU, while account shall always be taken of the operating and technical possibilities, such as the moment when the 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;
(c) a financial institution shall, under Article 16(2) of the AML Act, delay a UT in the following two cases:
    1. the financial institution shall delay a UT at its own discretion if the execution of the UT poses the risk that the seizure of proceeds from criminal activity or funds intended for financing terrorism may be frustrated or substantially impeded; in such a case, the financial institution shall immediately notify the FIU of the UT delayed;
    2. the financial institution shall delay a UT if the FIU requests it to do so in writing;
(d) a financial institution shall not delay a UT if it is unable to do so for operating or technical reasons (it shall immediately notify the FIU of this fact) or if delaying the UT could, according to a previous notice from the FIU, frustrate the processing of the UT;
(e) the period of delaying an operation pursuant to Article 16 of the AML Act shall be at most 120 hours; therefore, if during this period the FIU notifies the financial institution that it has forwarded the case to a law enforcement authority, the financial institution shall extend the period of delay, though at most by a further 72 hours. The total period for which a UT may be delayed is, therefore, at most 192 hours. In the case that, during the time of delaying 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 the "Code of Criminal Procedure"), the financial institution shall execute the delayed operation following the expiry of the set period. Prior to the expiry of the delay period, the financial institution may execute the operation only if the FIU notifies it in writing that, from the aspect of processing the UT, its further delay is not necessary. Weekends and bank holidays shall not be counted in the period for which a UT is delayed.

The start of the delay period of an operation pursuant to Article 16 of the Act shall be deemed the moment when the customer expresses their intention (will) to handle funds on an account. If the financial institution presumes that the customer is willing to execute a UT (handle funds) in the future, it shall take personnel, organisational and technical measures so that, in the event that the customer does give such instruction, it is not executed, thereby frustrating a potential delay of the UT.

The beginning of the period of delaying an operation pursuant to Article 16 of the Act may not be deemed the moment when the financial institution evaluated already-executed transactions as unusual, or learnt of the customer's executed operations. Likewise, a transaction

cannot be delayed solely because the customer asked the financial institution for general information regarding an account (information on the account balance, etc.).

Article 10

Measures against terrorist financing

(1) Terrorism represents one of the most serious violations of values such as human dignity, freedom, equality, solidarity, and respect for the 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 the Member States and on which the European Union is founded. The AML Act 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 addressed by the recommendations of the Financial Action Task Force (FATF). Further information on terrorist financing is available on the website of the FATF (http://www.fatf-gafi.org/publications/fatfgeneral/documents/terrorist financing.html).

(3) The International Sanctions Act defines an international sanction as a restriction, prohibition or instruction issued for the purpose of ensuring, maintaining or restoring international peace and security, the protection of fundamental human rights, combatting terrorism and the spread of weapons of mass destruction, and accomplishing the objectives of the EU's Common Foreign and Security Policy and those of the United Nations Charter.
The aim of sanctions is to ensure, maintain or restore international peace and security, to fight terrorism and the spread of weapons of mass destruction according to the principles of the UN Charter and the EU's Common Foreign and Security Policy.

(4) Procedures to be used in meeting the reporting duty:

(a) financial institutions shall implement a CFT framework in their relations with customers that is analogous to their AML policy, including the reporting to the FIU of UTs connected with terrorist financing;
(b) financial institutions shall report UTs to the FIU without undue delay (Article 17(1) of the Act); the Act defines a UT 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 who may be related to 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 applied under the International Sanctions Act;
(c) financial institutions shall, under Article 91(8) of the Banking Act, provide the Ministry of Finance of the Slovak Republic, within the time limits set by it, with a list of customers subject to international sanctions under the International Sanctions Act and the relevant decrees. The list must also contain 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 natural person or legal person to which international sanctions apply including:

(a) a country against which international sanction have been imposed;
(b) a citizen of a country against which international sanctions have been imposed;

(c) a dependant or representative of a person subject to international sanctions;
(d) other natural person residing in a country to which international sanctions apply, except for a citizen of the Slovak Republic;
(e) a legal person with a registered office in a country to which international sanctions apply; or
(f) a person included on the list of persons subject to sanctions issued by the Security Council of the United Nations or a person named in a decision issued under Title V of the Treaty on European Union or in the legal acts of the EU.

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

The regulations and decisions of the EU 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's Common Foreign and Security Policy (in the framework of enforcing the Common Foreign and Security Policy) are listed on the website at http://eeas.europa.eu/cfsp/sanctions/index_en.htm.

The relevant EU sanctions are available on the website of the Ministry of Foreign Affairs of the Slovak Republic (http://www.foreign.gov.sk/sk/zahranicna_politika/europske_zalezitosti-sankcie_eu, http://eeas.europa.eu/cfsp/sanctions/docs/measures_en.pdf).

The consolidate list of sanctions is available at the website: https://www.consilium.europa.eu/en/policies/sanctions/different-types.

(7) The inclusion of a person on the list of persons subject to sanctions, the removal of a person from that list, and the rights and duties of persons subject to sanctions in the conditions of the Slovak Republic are regulated by the provisions of Articles 16 to 18 of the International Sanctions Act.

(8) Financial institutions shall proceed in accordance with the procedures used for applying effectively the rules governing the freezing of financial assets of persons subject to sanctions in the Slovak Republic, which are available at the website: https://www.finance.gov.sk/sk/financie/financny-trh/bankovnictvo/sankcie-eu/.

Article 11

Archiving of data and documentation

(1) Financial institutions are entitled, for the purposes of performing customer due diligence (Articles 10 to 12 of the AML Act) and detecting UTs (Article 14 of the AML Act), without the customer's consent and without informing the customer concerned, to ascertain, acquire, record, store, use and otherwise process a customer's personal data and other data in the scope of the provisions of Articles 10(1), 11(3), and 12(1) and (2) of the AML Act.

(2) Financial institutions are entitled to acquire the necessary personal data of customers also by copying, scanning or otherwise recording official documents stored 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 aforementioned provisions of the AML Act.

(3) In entering into a business relationship or executing an occasional transaction, a financial institution shall warn the customer of the financial institution's obligation to process personal data for the purpose of money laundering and terrorist financing prevention (Article 21(3) of the AML Act).

(4) Under Article 19(1) and (2) of the AML Act, financial institutions are required to archive for a period of five years:

(a) from the end of the contractual relationship with a customer, data and written documents acquired by way of the procedure described in Articles 10 to 12 and Article 14 of the AML Act;
(b) from the execution of a transaction, all data and written documents concerning the customer.

(5) In view of the importance of the information acquired by financial institutions in fulfilling AML/CFT duties under Article 14(2)(a) of the AML Act, financial institutions are required to archive for the statutory period (five years from the written record being made) also written records of the assessment process.

(6) A financial institution shall archive such data and written documents also for longer than five years if the FIU requests it do so by way of a written request specifying the relevant period, which must not exceed another five years, and the scope of data and written documents to be archived.

(7) This duty applies also to a financial institution that ceases business, up until the expiry of the period during which it is required to archive such data and written documents.

(8) Financial institutions are required to adopt an effective system in line with their size and nature of activities, designed to promptly provide the FIU, NBS and law enforcement authorities, upon request, with data and documents on transactions or business relationships and with information on persons involved in any way in the transactions conducted.

(9) The procedure followed by a financial institution in archiving data and documentation, and records relating to AML/CFT shall be governed by the financial institution's Programme, which should, in accordance with the AML Act, set out in detail:

(a) the records that need to be archived;
(b) the form of records archived (paper, electronic);
(c) the place, manner and period for which records are to be archived, taking account of:
    1. the end of the contractual relationship with the customer;
    2. the execution of a transaction with the customer; and
    3. any written request of the FIU and the period specified in Article 19(3) of the AML Act.

(a) Records that need to be archived:

1. records on customer due diligence

Financial institutions shall archive data and written documents on customer due diligence they apply (basic, simplified enhanced) obtained by way of the procedure described in Articles 10 and 12 of the AML Act, on the identification and verification of customers and beneficial owners, politically exposed or sanctioned persons, and information on the purpose and planned nature of transactions. Documentation on facts about the origin of property and funds also needs to be archived when relevant to the risk of money laundering or terrorist financing.

2. records on customers' risk rating

Documents and information related to the assignment of customers to risk groups must be archived, too. Financial institutions shall record and archive important information confirming the circumstances justifying a customer's reassignment to a different risk group (and therefore change in the customer's risk profile) together with other data on the customer.

3. records on financial operations

The internal regulations of a financial institution should establish the duty to record all financial operations carried out for customers in the financial institution's accounting and reporting system. Records on financial operations that support accounting entries should be archived in a form that allows the FIU, supervisory authority, control authority and the law enforcement authorities to compile a satisfactory record and to verify each customer's risk profile. Supporting records shall also contain the customer's instructions related to the customer's payments. The financial institution shall archive records on each financial operation made by the customer, including single financial operations performed for customers who do not have an account at the financial institution. The archiving period in this case is the same as for archiving identification records and documents.

4. records on internal notifications of UTs and UT reports

Financial institutions shall archive all reports on a customer's unusual activities, namely internal notifications of UTs intended for the NO, as well as UT reports that the NO has sent to the FIU.

If, after assessing the relevant information and knowledge concerning a customer's unusual activity, the NO decides that this does not constitute a UT and so there is no need to report the case to the FIU, the reasons for that decision must also be recorded and archived, together with the records on the relevant transaction.

5. records on staff training and education

Financial institutions shall archive records on staff training focussed on familiarisation with the AML/CFT Programme, containing the names and positions of the participating employees, the date and place of training, and its form and content.

(b) Form of records

Archives must be kept of originals or photocopies of paper documents and documentation, as well as data stored in personal computers and on mechanical media in electronic form.

Copies of documents must be made in a manner ensuring that the relevant data are legible and suitable for archiving. A natural person's image copied from their identity document must be of adequate quality, enabling easy identification and verification.

(c) Place, manner and period for which records must be archived

Archiving periods are the same, regardless of the form in which the data are archived. In view of the need to provide additional data on customers and on their financial operations, particularly for the FIU, NBS and law enforcement authorities, it is important that financial institutions are able to find, without undue delay, the necessary data or records (in their archives of documents and data media). Financial institutions shall also continue to archive such information and documents on customers and their financial operations after the expiry of the statutory archiving period in cases where an investigation has been started by the competent law enforcement authorities, or a criminal prosecution has begun, for the purposes of investigation and criminal prosecution, on the basis of a written request received from the FIU pursuant to Article 19(3) of the AML Act; the scope and the additional period required must be stated in the request.

(10) Records prepared and archived by a financial institution shall satisfy the statutory requirements for keeping records of customer data and also enable:

(a) an independent party to evaluate the efficiency of compliance with the basic principles, as well as the financial institution's procedures regarding AML/CFT;
(b) reconstruction of the course of financial operations carried out by the financial institution for a customer;
(c) identification and location of each customer in the archives;
(d) identification of all internal notifications of UTs and reports on UTs to the FIU;
(e) fulfilment within a reasonable time of statutory requests received from the FIU, supervisory authority and law enforcement authorities concerning a customer, the customer's business relationships and transactions.

Article 12

Securing the control system and ensuring the performance of internal control

(1) The control system shall comprise a specification of control responsibilities at all levels of the management and performance of banking activities, as well as the performance of internal control by:

(a) the bank's supervisory board;
(b) members of the statutory body;
(c) the Nominated Officer (or their deputy);
(d) the senior managers;
(e) the staff involved in the processing of customers' instructions (financial operations);
(f) the internal control and internal audit unit.

(a) and (b) Control performed by the statutory body and the supervisory board

Control shall be based on legislation of general application and the financial institution's internal regulations and derived from the position in the hierarchy of the financial institution's management system. The financial institution's statutory body shall regularly, at least once a year, evaluate the effectiveness of the existing system – the AML/CFT policy, the Programme and specific measures, including the activities of the relevant units and staff.

(c) and (d) Control activity of the NO and that of senior managers

Control activity shall be based on the powers, duties and responsibilities of the financial institution's NO and senior managers, and shall be performed as a regular and continuous activity aimed at controlling the performance of work duties, consisting in the verification and

approval of the quality, level or status of the performance of work activities of the subordinate staff in the field of AML/CFT.

(e) Control performed by the staff

This represents a continuous control process in each unit of the financial institution, performed on a daily basis. It comprises control mechanisms that are a direct component of the staff's working procedures, as well as their work duties, tasks and responsibilities as front office staff arising from the AML/CFT policy.

(f) Internal control and internal audit

The internal control and internal audit unit shall control compliance with the Programme and internal regulations, and shall verify the AML/CFT procedures adopted and the performance of duties by staff members at various workplaces who execute, receive, or process instructions for customers' payment operations, as well as the performance of duties by senior managers and the NO (or by his deputy).

The performance of internal control should be focused primarily on checking:

1. the performance of customer due diligence in line with the customer's risk category;
2. the procedures used for ensuring that the information obtained on customers is up to date (verification);
3. the assessment of specific financial operations, monitoring of customers, their financial operations and business relationships;
4. risk assessment and management in the AML area;
5. internal notification of UTs and their reporting to the FIU;
6. the organisation of staff training; and
7. the storage of records, data and documentation.

(2) A financial institution's AML/CFT system and processes should be subject to internal audit, carried out at least once a year. The audit should evaluate the functionality, effectiveness and efficiency of all elements, tools, procedures, management and control mechanisms applied in this area.

(3) The members of a bank's statutory body and the head of a foreign bank branch should be regularly informed of the results of internal controls and audits performed, e.g. once a year and immediately in the event of a finding of serious deficiencies. An internal audit of this kind should be carried out in accordance with the tasks plan of the internal control and internal audit unit at intervals set according to an evaluation of the risks involved in the individual areas of the financial institution's activity.

PART III

Final provisions

(1) This Methodological Guideline replaces in full the Methodological Guideline of the Financial Market Supervision Unit of Národná banka Slovenska No 4/2009 of 20 November 2012 on the protection of banks and branches of foreign banks against money laundering and terrorist financing.

(2) This Methodological Guideline enters into force on the date of its publication in the Journal of Národná banka Slovenska.

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 the AML Act 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 customer due diligence measures in a way that is commensurate to the identified money laundering and terrorist financing risks.

The joint guidelines are available also in Slovak: (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 risk of money laundering and terrorist financing (hereinafter 'ML/TF') 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 the AML Act 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 obligatory 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:
(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:
(a) 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.)?
(b) 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)?
(c) Does the customer or beneficial owner have links to sectors that involve significant amounts of cash?
(d) 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)?
(e) 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)?
(f) 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:
(a) 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)?
(b) 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?
(c) 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:
(a) 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?
(b) 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.)?
(c) 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, is the customer trying to evade specific thresholds set out for occasional transactions)?
(d) 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)?
(e) Does the customer issue bearer shares as part of their business activity?
(f) 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)?

(g) 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?
(h) 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.

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:

The customer is not physically present for identification and verification purposes. For this type of establishment of a business relationship, financial institutions should have a procedure in place for a reliable form of non-face-to-face obligatory customer due diligence.

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 customer due diligence measures to EU standards in line with Article 21(4) and (5) of the AML Act.

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”.

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 basic 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 laid down by the AML Act, 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 product, service or transaction sought has features that limit its 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) the situations in points 1 and 2 do not result in an exemption from 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 mentioned in point 2 has been reached;
(d) they do not defer customer due diligence or delay obtaining relevant information about the customer needed.

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 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). If statutory thresholds are exceeded, financial institutions must perform basic customer due diligence.

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 a statutory 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 customer due diligence measures but must be applied in addition to regular customer due diligence measures.

Under Article 12 of the AML Act, financial institutions are obliged to perform enhanced customer due diligence where risk assessment under Article 10(4) of the AML Act indicates that a customer, transaction type or individual transaction 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 as presenting a high risk.

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 designated person under Article 20(2)(h) of the AML Act 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 financial institution's risk profile. 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 designated person under Article 20(2)(h) of the AML Act 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, it must apply enhanced customer due diligence measures.

These enhanced customer due diligence measures should be sufficient to help the financial institution determine whether these transactions give rise to suspicion of money laundering 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 the likelihood of the customer 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 or 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 or 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 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 designated person 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 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 shall 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, past compliance failures of employees 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 retail banks – Risk factors

For the purpose of these guidelines, 'retail banking' means the provision of banking services to natural persons and small and medium-sized enterprises. Examples of retail banking products and services include current accounts, mortgages, savings accounts, consumer and term loans, and credit lines.

Due to the nature of the products and services offered, the relative ease of access and the often large volume of transactions, cap-free transactions and business relationships, retail banking is vulnerable to terrorist financing and to all stages of the money laundering process.

Financial 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 allows payments from third parties that are neither associated with the product or service nor identified upfront, where such payments would not be expected, for example for mortgages or loans;
(b) the product or service places no restrictions on cash and cashless transactions, including cross-border transactions;
(c) new products or services and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and existing products or services;
(d) an unusually high volume or large value of transactions.

4.2 Customer risk factors

(a) the customer is a cash-intensive undertaking;
(b) the customer is an undertaking associated with higher levels of ML risk (for example certain money remitters and gambling businesses);
(c) the customer is an undertaking associated with a higher corruption risk (for example operating in the extractive industries or the arms trade);
(d) the customer is a non-profit organisation that supports jurisdictions associated with an increased TF risk;
(e) the customer is a new undertaking without an adequate business profile or track record;
(f) the customer's beneficial owner cannot easily be identified, for example because the customer's ownership structure is unduly complex or opaque, or because the customer issues bearer shares;
(g) the customer is reluctant to provide customer due diligence information;
(h) the customer's evidence of identity is in a non-standard form for no apparent reason;
(i) the customer's behaviour or transaction volume is unexpected based on the information the customer provided at account opening;
(j) the customer's behaviour is unusual (for example the customer unexpectedly and without reasonable explanation accelerates an agreed repayment schedule, by means either of lump sum repayments or early termination; deposits or demands payout of high-value banknotes without

apparent reason; increases activity after a period of dormancy; or makes transactions that appear to have no economic rationale).

4.3. 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.

4.4. Delivery channel risk factors

(a) financial institutions rely on a third party's customer due diligence measures in situations where the bank does not have a long-standing relationship with the referring third party;

(b) new delivery channels that have not been sufficiently tested yet.

Part 5
Sectoral guidelines for financial institutions providing private banking services – Risk factors

'Private banking' is the provision of premium banking and financial services to high-net worth natural persons (customers). Private banking customers are usually provided services through relationship management staff or the so-called private bankers who tailor the products or services to their individual needs. The provided services cover various area, including banking (payment accounts, credit cards, loans, etc.), investment advice and management, family office services, tax and estate planning, etc.

Many of the features typically associated with private banking, such as wealthy and influential customers; very high-value transactions; complex and structured products or services, including tailored investment products; and an expectation of confidentiality and discretion are indicative of a higher risk for money laundering relative to those typically present in retail banking.

Private banking services may be particularly vulnerable to abuse by customers who wish to conceal or provide minimum information about the origins of their funds.

Hence, the application of general AML measures by financial institutions providing private banking services may prove inappropriate and insufficient. Financial institutions should therefore reassess their approach to private banking customers and take adequate customised AML measures. The objective of these customised measures should be to decrease the vulnerability of the financial institution as a whole and of the provided private banking products or services.

Financial institutions should consider the following risk factors and measures with respect to private banking:

5.1. Customer risk factors:

(a) customers with income and/or wealth from high-risk sectors such as arms production and trade, the extractive industries, construction, gambling, casinos, etc.;
(b) customers who expect or require unusually high levels of discretion or confidentiality;
(c) customers whose spending or transactional behaviour makes it difficult to establish expected patterns of behaviour;
(d) very wealthy and influential customers, including customers with a high public profile;
(e) non-resident customers and politically exposed persons;
(f) customers about whom credible allegations of wrongdoing have been made.

5.2. Products, services and transactions risk factors:
(a) private banking customers requesting large amounts of cash;
(b) very high-value transactions;
(c) business taking place across multiple countries, particularly where it involves multiple providers of financial services;
(d) cross-border financial instruments where assets are deposited or managed in another financial institution, either of the same financial group or outside of the group, particularly where the other financial institution is based in a jurisdiction associated with higher ML/TF risk;
(e) financial instruments involving jurisdictions associated with higher ML/TF risk.

5.3. Country and geographical area risk factors:
(a) the customer conducts business in countries that have a culture of banking secrecy or do not comply with international tax transparency standards;
(b) the customer lives in, or their funds derive from activity in, a jurisdiction associated with higher ML/TF risk.

The following enhanced customer due diligence measures may be appropriate in high-risk situations related to the provision of private banking services:
(a) obtaining and verifying more information about customers than in standard risk situations and reviewing and updating this information both on a regular basis and when prompted by material changes to a customer's profile; financial institutions should perform reviews on a risk-sensitive basis, reviewing higher risk customers at least annually but more frequently if risk dictates;
(b) establishing the source of wealth and funds; where the risk is particularly high and/or where the financial institution has doubts about the legitimate origin of the funds; the source of funds or wealth can be verified, by reference to, inter alia, an original or certified copy of contract of sale of a company or investments; written confirmation of inheritance signed by a notary; original or certified copy of a will or grant of probate;
(c) performing greater levels of scrutiny and customer due diligence than would be typical in mainstream financial service provision;
(d) seeking senior management approval of business relationships with new and existing customers on a risk-sensitive basis;
(e) monitoring transactions on an ongoing basis; where necessary, reviewing each transaction as it occurs, to detect unusual or suspicious activity; monitoring measures may include the use of thresholds, and an appropriate review process by which unusual behaviours are promptly reviewed by relationship management staff;
(f) ensuring that cash (deposits, withdrawals) are handled only at bank counters or bank treasury, and never by relationship managers outside of the bank's premises;

(g) monitoring public reports or other sources of intelligence to identify information that relates to private banking customers or to their known associates, businesses to which they are connected or third-party beneficiaries to whom the private banking customer makes payments.

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 unusual signs 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, business relationship and transaction, it is necessary to take particular account of:

1. Information on the customers and circumstances of concluding the business relationship, or circumstances of the provided product, service or transaction, 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. Today, given the emphasis placed on electronic banking and the quantities of transactions made daily, practically 24 hours/7 days a week, a financial institution in identifying and assessing UTs cannot work solely from information provided by front office staff;
6. Information from the financial institution's registers established under the Banking Act;
7. Information received from other obliged entities;
8. Information from commercial databases;
9. Information from open sources;
10. Information arising from requests and instructions of authorised entities, in particular the police force, prosecutor, courts, executors, etc.;
11. 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;
12. Analyses and investigation results from AML group 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 execution of the transaction or purchase of a product or service;
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 a 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 the potential suspension of any UTs.

When detecting and assessing UTs, AML group 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 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 terrorism, etc.);
- Position as a politically exposed person;
- 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 is reluctant to present their identification or 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 (shell companies, 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 (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 (payment 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 account regime);
- Subject of the product, service or transaction (transactions related to high risk commodities);
- Coverage of the product, service or transaction;
- Method and form of payment;
- Documents presented by the customer;
- Customer's requirements;
- Business partners (more companies suspect of carousel fraud – payment 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, and products that it sells, 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:

- A person 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 features as the owner of several companies that have progressively been transferred to this person 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 acts alone;
- The presence of third persons who direct or check the actions of such a 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 intelligence services;
- Persons on lists of persons subject to sanctions,
- Persons on lists of terrorists or sympathisers of terrorism;
- Persons expressing through their appearance or statements sympathy to 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;
- 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, bureaus de change, trade in receivables, restaurant services and other operations working with cash;
- 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;
- The shell 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).

In relation to trusts (foundations, non-profit organisations providing services of general interest, non-investment funds):

- Discrepancy found between the value of transactions and the activities of the trust;
- The trust's finance is received fully or largely from abroad;
- A representative of the trust is a non-resident and large volume funds are directed from their home country and then transferred to foreign beneficiaries.

In relation to a product, service, transaction or request for their execution:

1. A product, service or transaction made by natural or legal persons associated with an increased risk of money laundering or terrorist financing;
2. 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;
3. A product, service or transaction in which the customer requests the establishment of a contractual relationship or execution of a business operation with the obliged entity on the basis of an unclear project;
4. A product, service or transaction in which the customer submits documents issued by a financial institution (mostly foreign) where the authenticity of such documents can be verified only with difficulty;
5. A product, service or transaction in which the customer submits false, invalid or stolen identification documents, forged banknotes, falsified documents or securities, etc.;
6. A product, service or transaction in the case of which the customer refuses to or cannot submit supporting documentation;
7. High-value cashless credit to the customer's account followed by cash withdrawals in amounts corresponding to the maximum unreported cash withdrawal;
8. Attempt by the customer to obtain credit for financing activities unrelated to the customer's line of business;
9. Use of money transfer service provided by the financial institution in parallel with ordinary payment services, despite it being disadvantageous for the customer;
10. Refusal to provide information on the basis of which, under ordinary circumstances, customers could obtain credit or other banking services;
11. Attempt by the customer to obtain credit where the source of the customer's financial contribution for the trade operation is unclear;
12. Repeated and frequent changes to the right of disposal on the basis of an authorisation granted by the account holder;

13. Repeated deposits by a large number of customers who make payments to the same account with no apparent purpose;
14. Attempt to perform transactions using various unknown guarantees and warranties;
15. Opening of accounts or performance of transactions, particularly for foreigners, through an authorised person;
16. Large sums of money transferred to or from abroad using payment services;
17. 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 upon which international sanctions have been imposed under a separate regulation;
18. 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.);
19. Fund transfers, via postal orders made by a representative of a legal person, to an account of a different legal person or natural-person entrepreneur;
20. Payment of an excess of VAT deduction, or other payment from a state treasury account (usually to a newly opened account, an account not registered by the tax administrator, or unused for a long period) and its immediate withdrawal in cash or transfer to another account and subsequent withdrawal in cash, or subsequent immediate change in the form of funds, e.g. to investment in securities, etc.;
21. Transactions on a personal account that have the nature of a business activity or are linked to such activity, where these actions may be masking illegal income since the customer creates the impression that they constitute management of personal finances;
22. High growth in account balances that is not in accordance with the customer's known and normal turnover, and their subsequent transfer to an account (or accounts) abroad;
23. A significant increase in cash or negotiable securities deposits by a legal person, with the use of accounts of a different customer or the legal person's internal accounts or holder's accounts, in particular where the deposits are immediately transferred between a different company of the customer and the holder's accounts;
24. A request by a customer for investment (securities) management services, where the source of funds is unknown or not consistent with the customer's apparent, in particular financial, situation;
25. 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, change of registration court, etc.;
26. 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;
27. A cash deposit to an account and subsequent request by the customer to issue a confirmation of the current account balance, followed by a withdrawal from the account;
28. Number of movements on an account in one day or consecutive days which goes beyond the ordinary scope of the customer's financial operations;
29. Cash deposit or transfer abroad, where the customer states the payment purpose as a fee or commission;
30. Unusually high deposit of funds to an account of a natural person who is a foreign politically exposed person, and which goes beyond the ordinary scope of movements on that account;

30a. Several cash withdrawals in one day (or consecutive days) from more bank branches in the maximum amount or limit set by the bank for unreported cash withdrawals.

Methods of money laundering or terrorist financing via 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 accounts of natural persons or legal persons, followed by their immediate withdrawal or transfer of almost the whole credited amount, 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, CEO fraud, payment card fraud, payment terminal fraud;
3. Placing proceeds from crime on bank accounts in tax havens or on accounts of companies registered in offshore areas; the account may be set up virtually anywhere;
4. Transfers between companies with an unclear ownership structure that do not have any apparent economic basis or reason;
5. Dealing in arms and hazardous materials that are covered by fake trades made by companies domiciled in a tax haven, with local accounts used only for transfer and for obscuring financial flows;
6. Misuse of lawyers' or notaries' customer accounts, the primary objective not being to provide services, but to create a credible source of funds;
7. Reverse loan, most often using accounts of foreign natural or legal persons, usually domiciled in a tax haven;
8. Investment by foreign entities committing crime in Slovakia and vice versa. This concerns particularly investment in real estate, securities, high-value goods and the purchase of shares in companies;
9. 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;
10. Use of domestic and foreign accounts, in particular those of natural persons, for on-line betting and online gambling;
11. Loading of a player's account via anonymous prepaid cards and a subsequent transfer of funds from the player's account to a personal account (or an unauthorised loading of a player's account via other, most frequently foreign payment cards), without actual participation in the game;
12. Use of Slovak and foreign legal persons' company accounts to transit funds through Slovakia.

Forms of UT may involve in particular:

A. Private banking

1. A product, service or transaction in which the customer refuses to provide information on an 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 great cost;
2. 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 account movements do not correspond to the nature or scope of the customer's business activity or usual financial operations;
3. A one-time cash deposit to an account that does not correspond to the customer's hitherto activities and information that the financial institution has available on the customer;
4. 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;

5. Frequent cash deposits to an account used for covering bank drafts, money transfers or for other negotiable and highly liquid instruments;
6. Unusually high cash deposits made by a natural or legal person in the business activities in which cheques and other instruments would normally be used;
7. Customer activity relating to the opening of multiple accounts, the number of which is in clear disproportion to the line of business, and the related transactions between these accounts;
8. Cashless deposits by third parties and subsequent cash withdrawals of the funds by the customer for purposes for which other forms of payment, e.g. cheques, letters of credit, bills of exchange, are normally used;
9. Frequent deposits of large quantities of low-denomination banknotes to an account;
10. Frequent exchanges of large quantities of low-denomination banknotes for higher-denomination banknotes;
11. Frequent exchange of cash for other currencies (attempt to conceal the origin of the money through conversion to a different currency);
12. Transactions of a customer who promises their customers unusually high returns;
13. Use of letters of credit and other forms of payment usual abroad, in cases where such forms of payment are not usual in the customer's known business activities;
14. Request for a loan against assets held by a financial institution or a third party, where the origin of those assets is not known or the assets do not correspond to the customer's situation;
15. Provision of a loan that is secured by a cash deposit in a foreign currency by a third party that is not known to the financial institution in the same scope as the customer to whom it provided the loan;
16. Securing a loan by funds "in cash", i.e. deposited on deposit accounts, or deposits in passbooks;
17. Early repayment of a provided loan, particularly where the origin of the funds from which the customer early repaid the loan is unclear or where the customer in the past had loan repayment problems;
18. Repeated back-transfers of funds to foreign banks domiciled in high-risk areas or to companies domiciled in high-risk areas;
19. Purchase and sale of securities outside the customer's normal practice without proper justification;
20. Large cash deposits through night-safe deposit services, where it is possible to avoid direct contact with staff;
21. Withdrawals of large amounts of money from a previously sleeping or inactive account, or from an account to which an unexpectedly high deposit had just been transferred;
22. Increased activity of natural persons in frequent use of night-safe deposit services;
23. Rental of a safe-deposit box to which multiple persons have access whose personnel, business or other similar connection is not known;
24. Purchase of traveller's cheques in cash and their subsequent sale to the financial institution;
25. The use of letters of credit and other forms of documentary payment by customers who had not previously used in their business activities letters of credit or other payment instruments, and who began to use these payment instruments to a greater degree within a certain period without giving proper reasons;
26. High or unusual settlement of securities in cash;
27. Purchase and sale of securities without discernible purpose or under circumstances that seem unusual;

28. Any transaction with a broker where the identity of the beneficial owner or counterparty is secret, contrary to standard practice for the given type of a product, service or transaction;
29. Products, services or transactions involving newly-incorporated companies registered in tax havens;
30. Repeated back-transfers of funds to and from foreign banks domiciled in high-risk areas;
31. Transactions relating to acts by notaries and lawyers on behalf of customers, e.g., a payment from abroad, outside the EU, and its withdrawal in cash and subsequent closure of the account;
32. Involvement of a firm or financial institution from a high-risk country in a transaction.

B. Retail banking

1. Cashless credit in a high amount to the customer's account followed by cash withdrawals in amounts corresponding to the maximum unreported cash withdrawal;
2. Cash withdrawal in an amount that does not fit the framework of the customer's ordinary withdrawals;
3. Repeated and frequent changes to the right of disposal on the basis of an authorisation granted by the account holder;
4. A large number of people who make payments to the same account without adequate explanation;
5. Cash withdrawals immediately following receipt of a payment from a state treasury account, or transfer of such a payment to a different account with subsequent cash withdrawal;
6. Payment of an excessive of VAT deduction, usually to a newly-opened or sleeping account, and its immediate withdrawal in cash;
7. Transactions on a personal account (e.g., large volume payments or transactions related to a company account (or accounts));
8. Accumulation of substantial funds within one day or consecutive days acquired through a combination of cashless and cash transactions;
9. High growth in account balances that is not in accordance with the known turnover of the customer's company and their subsequent transfer to an account (or accounts) abroad;
10. Payment of a commercial nature between two customers of the same branch made as two transactions, namely a cash withdrawal and subsequent cash deposit, usually without movement of the cash;
11. Attempt by the customer to enter into a contractual relationship with the financial institution or to perform a transaction on the basis of unclear projects, or to open an account with the minimum balance, with a request for a confirmation of the account balance;
12. Electronic and cash operations with larger volumes between personal and company accounts which are declared as mutual loans and credits.

C. Electronic – internet banking

1. Cashless credit of a high amount to the customer's account followed by cash withdrawals by payment card in amounts corresponding to the maximum unreported cash withdrawal;
2. Customer transferring large sums of money abroad or from abroad clearly at variance with the information available to the financial institution;
3. Payment from abroad, particularly outside the EU, and its immediate cash withdrawal by payment card;
4. Payment from abroad, particularly outside the EU – with the payment purpose: donation;

5. 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;
6. Frequent changes in the telephone number used to receive the system-generated SMS code necessary for the identification of the customer when executing transactions on their account;
7. Transfer of funds from the account made immediately after the funds were received from a different account;
8. Transactions executed in connection with the performance of business activity (payments for illegal goods, fictitious invoices, VAT payments/refunds from the state treasury);
9. 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;
10. Operations made on an account where payments are in low nominal values, though in an extraordinarily high total volume;
11. Frequent ATM cash withdrawals, even at the cost of increased charges for individual withdrawals;
12. One telephone number for receiving an SMS code (generated by a bank system and necessary for the customer identification) which the bank system registers with several customers with no obvious relation.

D. Investment banking

1. Cashless deposits by the customer and third parties and subsequent cash withdrawals of the funds by the customer for purposes for which other forms of payment, e.g. cheques, letters of credit, bills of exchange, are normally used;
2. Payments by the customer in cash for payment of bank drafts or other negotiable securities;
3. Letters of credit and other methods of financing the product, service or transaction are used to move money between countries, where such product, service or transaction is not consistent with the customer's normal business activity;
4. Frequent requests for traveller's cheques, foreign currency drafts or other negotiable securities that are not consistent with the customer's normal business activity;
5. A request by the customer for investment (securities) management services, where the source of funds is unknown or is not consistent with the customer's apparent situation;
6. Use of letters of credit and other forms of payment usual abroad, in cases where such forms of payment are not usual in the customer's known business activities;
7. Purchase of traveller's cheques in cash and their subsequent sale to the financial institution;
8. Use of letters of credit and other forms of documentary payment by customers who had not previously used in their business activities letters of credit or other payment instruments, and who began to use these payment instruments to a greater degree within a certain period;
9. Settlement of securities in cash, which is not in accordance with the customer's apparent situation;
10. Purchase and sale of securities without discernible purpose or under circumstances that seem unusual;
11. Execution of transfers of funds in connection with investing in real estate, securities, high-value goods and purchase of shares in companies.

E. Housing saving

1. Early repayment of a loan on a housing saving account, on which the customer had in the past been recorded as insolvent;

2. Repayment instalments to a housing saving account from accounts of legal or natural persons, the account holder of which is not the saver, or from multiple accounts;
3. Termination of a housing saving contract with payment of the account balance to an account different from that from which regular repayment instalments were made;
4. Payment of balances from several housing saving contracts of different customers to the same account number;
5. Multiple repeated changes during the course of a year to a saver's account for payments or repayment of housing savings;
6. High volume payments to several housing saving accounts of the same customer, with the funds being deposited on the accounts in cash;
7. Payment of saving instalments by the customer exclusively in low-denomination banknotes;
8. Payment of instalments in a lump-sum exceeding €15,000 per contract;
9. Payment of saving instalments by transfer from accounts registered offshore;
10. Request by the customer for return of a payment sent to a housing saving account erroneously, though the customer requests that payment be made to an account different from that from which the payment was made.