Methodological Guideline
of the Financial Market Supervision Unit of Národná banka Slovenska
No 6/2019 of 13 May 2019
regarding protection against money laundering and terrorist financing
in relation to the activity of an investment firm, a branch of a foreign investment firm,
a management company, a pension funds management company,
and a supplementary pension management company

The Financial Market Supervision Unit of Národná banka Slovenska (hereinafter the "NBS"), on the basis of Article 1(3)(a) point 3 of Act No 747/2004 on financial market supervision, as amended, in collaboration with the Ministry of Interior of the Slovak Republic, the Financial Intelligence Unit (hereinafter the "FIU"), in order to ensure the uniform procedure for the performance of duties arising from the prevention of money laundering and terrorist financing (AML/CFT), has issued this Methodological Guideline:

PART I

Article 1
Subject matter and purpose

(1) This Methodological Guideline aims to provide explanation to companies carrying out investment services and investment activities, old-age pension scheme and supplementary pension scheme and collective investment for fulfilling their duties arising under legal regulations focused on the prevention of money laundering and terrorist financing (hereinafter the "AML/CFT") in the financial system. The legal regulation in this area is complex as it is based not only on Slovak legislation but also on international standards, on knowledge, experience and practice gained in the performance of supervision by the NBS and control by the FIU.

(2) This Methodological Guideline reflects the findings and conclusions of the national risk assessment in this area, which the Slovak Republic is required to carry out in accordance with the provisions of Directive (EU) 2015/849. The overall vulnerability of the sector – the capital market was assessed at a medium-low level, which is 0.37.

(3) The purpose of this Methodological Guideline is to clarify and specify in more detail the procedure of the NBS in the exercise of supervision, which will apply and interpret the basic obligations and tasks arising in this area, the criteria under which it will assess compliance with legal provisions as well as compliance with the rules ensuring AML/CFT in the area of capital market.

(4) The preparation of this Methodological Guideline was based on the fact that the rules laid down by legal regulations, in particular by the law implementing Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, are only minimum requirements and cannot, with their content, provide guidance on how to deal with all cases that arise in practice. However, the rules give the freedom to use other sources of information and to set own rules, if necessary stricter than those required by Slovak legal regulations. In accordance with

the purpose pursued by the above laws and this Methodological Guideline, it is also possible to use more advanced procedures, in particular those already in use and validated in practice.

(5) The purpose of Methodological Guideline is to define, clarify or explain the content of terms related to the obligations imposed in the AML/CFT and thereby helping to create its own programme to combat money laundering and terrorist financing.

Article 2
Definitions

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

Investment firm	legal entity domiciled in the Slovak Republic, established as a joint stock company pursuing activity in the Slovak Republic under Article 54(1) of the AoSIS
Branch of a foreign investment firm	branch of a foreign investment firm pursuing activity in the Slovak Republic under Article 54(5) of the AoSIS
PFMC	pension funds management company whose establishment and operation are governed by Act No 43/2004 on the old-age pension scheme
SPMC	supplementary pension management company whose establishment and operation are governed by Act No 650/2004 on the supplementary pension scheme
MC	management company and foreign management company whose establishment and operation are governed by Act No 203/2011 on collective investment
Financial institution or company	all the above-mentioned financial institutions collectively – investment firm, branch of a foreign investment firm, PFMC, SPMC, MC and foreign MC
AoSIS	Act No 566/2001 on securities and investment services (and amending certain laws), as amended.
AoOAPS	Act No 43/2004 on the old-age pension scheme (including amendments to certain laws), as amended
AoSPS	Act No 650/2004 on the supplementary pension scheme (and amending certain laws), as amended;
AoCI	Act No 203/2011 on collective investment, as amended;
Act	Act No 297/2008 on the prevention of money laundering and terrorist financing (and amending certain laws), as amended;
AoIIS	Act No 126/2011 on the implementation of international sanctions, as amended
AML or AML area	area governed by the Act and AoIIS

FIU	Financial Intelligence Unit of the National Criminal Agency of the Police Force Presidium of the Slovak Republic
UT	unusual transaction
Employee	employee of a financial institution fulfilling the tasks defined by the Act
Legalisation	legalisation of proceeds from criminal activity
NO	the Nominated Officer pursuant to Article 20(2)(h) of the Act
KYC	the Know Your Customer principle
FATF	Financial Action Task Force, a leading institution in determining international standards to combat money laundering and terrorist financing at the global level
NRA	national risk assessment in the AML/CFT area

Article 3
Dirty money and legalisation

(1) The term "dirty money" means the money coming from a criminal activity or any assets obtained through a criminal activity (gains, income, proceeds from criminal activity, assets of non-financial nature with monetary value, e.g. intellectual property, etc.). The process of transformation of such illegal financial and non-financial sources into legal sources (by creating the impression of lawful acquisition of property) is called money laundering.

(2) Legalisation means the activity aimed at disguising the illegal origin of funds and creating the impression of their legal acquisition with a view to create the impression that the money was obtained in accordance with legal standards and to facilitate their reinvestment in legal economy, and it consists mainly in:

1. transformation or transfer of income or other property, conscious that such property comes from criminal activity, for the purpose of concealing or disguising the illegal origin of the property, or for the purpose of assisting the person who participated or participates in such an activity in escaping legal consequences of their action,

2. concealing or disguising the real nature, sources, placement, disposal and movement of property or change of rights related to the given property, conscious that such property comes from criminal activity,

3. acquisition, possession or disposal of proceeds or property referred to above, conscious of the real origin or the original owner or with the aim to conceal or frustrate the possibility of their identification,

4. association of persons for the purpose of committing the activity referred to above.

(3) All financial institutions whose activity is regulated by this Methodological Guideline are, in the course of their operation, exposed to the risk that the customers will misuse their services

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

PART II

Protection against money laundering and terrorist financing in operation of a financial institution

Article 4
AML/CFT policy

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

(2) In setting and applying the AML/CFT policy a suitable tool and valuable source of information are Slovak and international standards, opinions and guidance by Slovak and foreign regulators, analyses by major Slovak and foreign institutions or consultancy firms, and not least also the experience and the approach of other companies. In creating the AML/CFT policy, a financial institution also takes into account its business objectives and business plan, the existing clientele, geographic risks in relation to customers and financial instruments, range of provided services, method of providing the services in relation to individual financial instruments and related potential threat of their misuse for the ML/TF purposes.

(3) The AML/CFT policy forms a part of risk management, with particular relevance to operational risk management.

(4) Important components of the AML/CFT policy are, in particular, its own activity programme pursuant to Article 20 of the Act (hereinafter referred to as the "Programme"), an organisational structure ensuring effective and independent performance of AML activities, articles of association defining the competences and responsibility for the given area, as well as information intended for customers and the general public containing 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.

Article 5
Employees responsible for implementing AML/CFT tasks

(1) The statutory body of the financial institution is responsible for the financial institution's overall AML/CFT prevention and for implementing the AML/CFT policy, and it also adopts the AML/CFT policy in its written form.

(2) Responsibility for the overall AML/CFT prevention of the branch of a foreign financial institution (an investment firm, a management company) and implementation of the AML/CFT

policy lies with the head of the branch (hereinafter referred to as the "Responsible Person of the branch") who also adopts the AML/CFT policy in its written form. Responsibility for the practical implementation of activities in the field of AML, primarily the performance of day-to-day activities ensuring the implementation of the AML/CFT policy, reporting of unusual transactions and for ongoing contact with the Financial Intelligence Unit in the financial institution lies with the NO.

(3) Where the NO is not a member of the statutory body, its position in the financial institution should be ensured so that the nominated officer has the possibility to communicate directly with the statutory body and supervisory body of the financial institution and has access to the information and documents which the financial institution acquired by the company while performing customer due diligence.

(4) The NO and deputy NO of a financial institution are appointed and dismissed by the statutory body which ensures full substitutability for the post of the NO, by nominating a deputy, taking into account its personnel capacities, the size and range of the provided services.

(5) It is appropriate to provide performance of AML activities (practical implementation of AML) by internal capacity within the financial institution. Where a financial institution decides to outsource AML activities, it is appropriate to outsource the performance of such activities from a bank within the financial group in which it operates, so that the material, personnel and organizational prerequisites for the performance of the AML activity are fully met; this does not apply to the NO whose position within the financial institution is defined by law. The outsourcing of AML activities is without prejudice to the full liability of the financial institution in the AML field.

(6) In filling the posts of the NO and deputy NO and employees responsible for the AML field who will conduct financial operations in direct contact with customers, the financial institution requires the candidates to demonstrate civic integrity, appropriate AML training and appropriate professional experience, depending on the services provided and the activities performed. Civic integrity is to be demonstrated by the persons concerned by an extract from the Criminal Records Register. The financial institution ensures that the relevant employees have criminal liability from the infringement of AML legislation and standards.

(7) The NO of the branch of a foreign financial institution is appointed and dismissed by the Responsible Person or the head of the branch to whom the NO is fully subject.

(8) The NO is responsible mainly for:
(a) ongoing preparation and updating of the Programme and any other necessary regulations and procedures for the AML field;
(b) the performance of management and control tasks in the AML field that he performs and for which he is responsible;
(c) communication, cooperation and maintaining ongoing contacts with the Financial Intelligence Unit, including the timely reporting of any unusual transactions;
(d) organisation and setting of rules for the training of relevant employees, including new employees;
(e) analytical and advisory activity in relation to the assessment and reporting of unusual transactions by the respective employees in connection with the execution of customers' products, services and transactions.

(9) The NO and his deputy are required to perform their duties with due diligence.

(10) The NO prepares and submits a report on his activity to the statutory body at least once a year. The NO of the branch of a foreign financial institution prepares and submits a report on his activity to the Responsible Person of the branch and to the head of the branch also at least once a year.

(11) The activity report of the NO contains in particular the following information:
(a) statistics and a brief description of unusual transactions reported by employees to the FIU;
(b) statistics and a brief description of unusual transactions reported by employees that were not forwarded to the FIU, with reasoning, and;
(c) overview of identified deficiencies and draft measures and deadlines for their rectification;
(d) information from inspections carried out;
(e) information or overview of relevant employees' trainings conducted.

(12) An important element of the NO protection concept is to ensure that the NO and his deputy have a sufficiently independent status in the structure of managers and organisational units. The NO must have an independent status in the employees' organisational structure of the financial institution. Classification of the NO among managers in the financial institution's organisational structure contains the following elements guaranteeing an appropriately defined status of the NO and his deputy:
(a) arrangement of powers and duties of the NO and his deputy as of a manager in their job descriptions, with emphasis on the primary area of their operation, which is to ensure protection of a financial institution against money laundering and terrorist financing;
(b) separation from units responsible for executing customers' products, services and transactions;
(c) unlimited access of the NO and his deputy to all documents, databases and information at the financial institution;
(d) autonomous and independent decision-making of the NO and his deputy in assessing the suspiciousness of customers' transactions reported by the respective employees in the framework of the internal reporting system;
(e) autonomous and independent decision-making on the sending of unusual transaction reports to the FIU;
(f) control function of the NO and his deputy in relation to units and respective employees responsible for executing customers' products, services and transactions;
(g) separation of the NO (his deputy or Prevention Unit) from the internal control (if applicable) and internal audit unit in the organisational structure (while preserving follow-up inspection of their activity conducted from the side of the internal control or internal audit unit), which means that the function of the NO and his deputy must not coincide with the function of the financial institution's internal controller, but the accumulation of powers in the compliance function or in other functions is not exempted, except for the function of internal auditor;
(h) cooperation with the compliance and internal audit employees in the new types of products, services or transactions; as well as the powers to participate in the process of commenting on or evaluation of the new types of transactions (products, services) under preparation at the financial institution in terms of the risk related to money laundering and terrorist financing, new ways of providing customer due diligence (e.g. pursuant to Article 8 (a)) and to express a dissenting opinion to introduced new types of products, services and transactions or a new way in the case that they represent a disproportionate exposure to this risk;
(i) in the case of extraordinarily serious circumstances or situations, immediate information to a member of the statutory body, or the Responsible Person;

(13) An appropriate definition of the NO and his deputy's status as stated under (g) and (h) is ensured proportionally to the size of the financial institution, the nature, scale and complexity of the services provided, and the activities carried out, and to the functions actually established therein.

(14) The financial institution is required to verify the integrity of its future as well as current employees responsible for the AML field. Before an employee enters employment or a function where he will be in direct contact with customers, the financial institution has to ensure verification of the future employee in a sufficient manner (e.g. based on an excerpt from the Criminal Register). It is also possible for a financial institution to request a different form of proof of integrity, for example, by a reference letter from a previous employer, or by a performance appraisal of its future employee.

(15) The financial institution should on its trainings in the AML field regularly notify its employees responsible for the AML area of the criminal liability from the infringement of AML legislation and standards so that its employees are aware of it.

(16) In the framework of the NRA results and the follow-up steps in the action plan, the financial institution in order to mitigate the above risk should develop an internal rule for preventing conflict of interest which should also include the respective warning about the criminal consequences of actions of the persons responsible for the AML field infringing the AML legal regulations in force.

(17) The financial institution should intensify education and training of its employees responsible for the AML field, and thereby raise general awareness in the event of failure to comply with their obligations arising from legal regulations governing the AML area.

(18) The financial institution should perform the above tasks adequately to its size, number of customers, type and complexity of the financial instruments and operations provided as well as the scope of its activities.

Article 6
Programme of own activity

(1) Pursuant to Article 20 of the Act a financial institution draws up a programme of own AML/CFT activity (hereinafter referred to as the "Programme") as an internal regulation to be approved by the statutory body. The Programme is based on acts of general application, in particular the Act and other applicable laws mentioned in the introduction to this Methodological Guideline, Methodological Guideline of the FIU published and regularly updated on the website of the FIU (http://www.minv.sk/?Metodicke-usmernenia-a-stanoviska-FSJ) as well as on international standards – 40 FATF Recommendations.

(2) The Programme also takes into account the financial institution's AML/CFT policy and represents a transposition of the AML/CFT policy into practical principles, tasks, procedures, duties and responsibilities in the fields of AML and prevention of terrorist financing. Programme also contains specific authorisations, duties, responsibilities and tasks of the NO and relevant employees of the financial institution in the performance of activities, types of products, services and transactions for customers in terms of statutory requirements (in particular Article 20(2) of the Act) that require AML/CFT prevention, as well as the control powers of these subjects and control powers of employees performing compliance and internal audit. The Programme contains not only information on statutory provisions, employees' responsibilities, but also all operational procedures and duties of employees at the financial institution in the performance of the relevant type of customers' products, services and transactions, as well as the most common forms of UTs at the given financial institution. The Programme also defines information flows, information systems, control processes and mechanisms in this field.

(3) In creating its own Programme, the financial institution takes into account its own specific characteristics, in particular its size and market share, organisational arrangement, the type and range of permitted and performed activities and services, the types of transactions in relation to individual financial instruments and their range and specifics, the type and number of customers and the specifics and range of these customers' operations.

(4) In addition to the general elements defined in Article 20 of the Act, the Programme contains in particular:
(a) the specification of tasks, duties and exact definition of responsibilities and related competences arising from comprehensive AML/CFT prevention at the individual levels of management from the board of directors of the financial institution, or from the Responsible Person of the branch of a foreign investment firm down to the units of first contact with the customer, including the Prevention Unit, with the definition of the NO pursuant to Article 20(2)(h) of the Act;
(b) the nomination of the NO pursuant to Article 20(2)(h) of the Act, taking into account the NO's classification in a financial institution's organisational structure;
(c) the specification of person (persons, where appropriate) responsible for assessing whether an imminent or conducted transaction is unusual, the specification of the time when the assessment is to be performed (where possible, always before the execution of the transaction or in the process of its preparation), the specification of the method of performing assessment, i.e. to state what needs to be performed in an 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 result;
(e) the exact specification of the procedure for 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 law-enforcement bodies;
(f) the specification of basic tasks of the respective employees at all levels of management, the detection of UTs and the reporting of internal notifications of UTs to the NO (possibly also a specimen form for internal notifications of an UT) and the manner of ensuring the protection of the respective employees in connection with the UT they identified and reported to the NO;
(g) the obligation to identify customers in providing products or services or conducting individual transactions and the duty to verify this identification (verification);
(h) the obligation to record the identification made and the verification of customer's identification, as well as all financial operations executed for customers;
(i) the obligation to store records on customer identification and on the verification of their identification and on the financial operations conducted by customers, and this for the period set out by the Act;
(j) an overview of known types of unusual transactions, broken down by activity and type of product, service and transaction executed;
(k) the evaluation and management of risks associated with money laundering and terrorist financing under Article 20a of the Act, 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 the type of product and service and the type of transaction and accounts, as well as the risk category of customers;
(l) pursuant to Article 10(4) of the Act, the specification of the nature and extent of the implementation of customer due diligence on the basis of a risk evaluation results and risks consideration pursuant to Article 20a(1) of the Act;
(m) more detailed signs of unusualness by which a customer's unusual transactions can be recognised;
(n) the method and scope of feedback within the financial institution on internal notifications of unusual transactions;
(o) the procedure of the competent employees and NO in delaying an unusual transaction under Article 16 of the Act;

(p) the content and timetable of employees' training, training employees for performing AML/CFT tasks in the performance of particular financial and business activities, types of customers' products, services and transactions;
(q) the obligation to maintain confidentiality regarding an internal notification of an UT and its reporting to the FIU and regarding measures performed by the FIU (Article 18 of the Act), primarily in relation to the customer concerned, as well as toward persons having a certain relationship to 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 beneficial owners associated with the operation), as well as toward third parties, other than exceptions defined by the Act;
(r) measures and control mechanisms (the four eyes principle, restricted access) preventing the abuse of position or function by the respective employees to knowingly engage in money laundering or terrorist financing in the exercise of their function;
(s) the method and periods for storing information and documentation;
(t) an internal control system focused on AML/CFT, consisting of control mechanisms, process controls of managers, including controls by the NO and internal audits;
(u) definition of information flows and description of information systems focused on the collection, processing and reporting of information for AML/CFT, including regular reports submitted to the board of directors and supervisory board of the financial institution and Responsible Person of the branch, or head of the foreign branch.

(5) In creating its own Programme, the financial institution takes into account its own specific characteristics, in particular:
(a) its articles of associations and prevention policy;
(b) authorisations, duties, responsibilities and tasks of the NO, internal control unit and internal audit unit focused on AML/CFT and employees of a bank and branch of a foreign bank branch in the performance of banking activities and types of transactions;
(c) information flows, information systems, control processes and mechanisms in this area.

(6) The AML/CFT issue requires that the Programme is drawn up as an integral internal regulation accessible to all the financial institution's employees at least via an internal computer network.

(7) It is necessary to update the Programme not only in the case of a change in the relevant acts of general application, but also in the case of changes concerning the own performance of activities and types of products, services or transactions, before new or innovative technologies and software solutions for products and services are introduced (e.g. remote identification and verification of the customer) as well as in the case of changes to the financial institution's organisational arrangement, if such change may increase the ML/TF risk.

Article 7
Employees' awareness and training

(1) The persons responsible for the AML area in the financial institutions must be aware and have to make other employees concerned aware of the fact that the actual assisting, any knowing or unwitting involvement or involvement through negligence in money laundering or terrorist financing represents certain operational risk. By performing operations with proceeds or funds from any criminal activity, a financial institution may suffer damage or loss of reputation (reputational risk), and it may ultimately suffer significant financial losses.

(2) Success in applying an ongoing AML/CFT process depends on effective employees' training and their proper familiarisation with duties and powers in the area of AML. The statutory body of a financial institution, jointly with the NO, must ensure that employees are aware of the financial institution's responsibility, as well as aware about the personal liability of employees and their protection in identifying UTs in this area.

(3) A financial institution publishes in an appropriate manner information for employees as regards who performs the function of the NO and who deputises for the NO.

(4) A financial institution determines in its own Programme the optimal regime and method for informing its employees about the AML/CFT system and related procedures, duties and powers in AML/CFT, making the Programme and any other relevant regulations available to the respective employees, and organising regular staff training and educational activities for employees; whether regular training or other education activities, e.g. e-learning.

(5) The financial institution, in informing and training employees, takes account of its conditions, in particular its size and organisational arrangement, activities and types of products, services and transactions performed for customers, so that all necessary information reaches all employees for whom the information is intended. The model for performing employees' training has to be effective, flexible and fulfil the desired objective; therefore, it is essential that it is updated with regard to changing conditions. In the dynamics of the training process it is necessary to apply the conclusions of the NRA both in terms of organization and content. In a financial institution, updates and improvements should be set so that the status of the training process is at any time horizon appropriate to the ML/TF to which is the financial institution exposed.

(6) The effectiveness of a financial institution's AML/CFT prevention depends in large part on the level of knowledge of management bodies and employees of the financial institution about the given problem, consisting in familiarisation with basic legal regulations, the Programme and other related internal regulations of the financial institution. The diversity of the performed investment services and activities, auxiliary services and types of transactions, delivery channels through which the financial institution provides its services and, in particular, the diversity in the structure of customers give rise to varying degrees of risk and different techniques of money laundering or terrorist financing. The relevant employees (staff of first contact with the customer) must have all necessary information on the performed investment services and activities, auxiliary services and types of transactions which they will execute for customers and they must learn as soon as possible the criteria (signs of unusualness) for assessing or detecting unusual transactions. These employees must be able to assess the conduct of the financial institution's customers, as well as the content of financial operations performed by customers in terms of their degree of risk, unusualness or suspiciousness. Employees training should significantly contribute to employees acquiring the prerequisites for mastering procedures for applying the Know Your Customer principle (hereinafter referred to as the "KYC") and for recognising the degree of risk from the customer's actions, also with regard to the customer's categorisation into one of the three groups for mandatory customer due diligence (basic, simplified and enhanced due diligence). The relevant employees are an important element for preventing the misuse of the financial institution for money laundering or terrorist financing. Likewise, however, they can also be its weakest element, if they do not fulfil the set duties, or if they knowingly or unwittingly participate in the execution of a customer's unusual transactions.

(7) In the framework of training, the financial institution ensures that employees are familiarised with the consequences of negligence or negligent fulfilment of their work duties and of any knowing or unwitting participation in money laundering or terrorist financing, as well as the consequences of a breach of the prohibition of providing a customer with information to which the

duty of confidentiality applies (Article 18 of the Act); as well as with the manner of their protection in the case of detecting an unusual transaction.

(8) The financial institution must have a project or plan of employees training, taking into account the employee's work classification (own categorisation according to job positions, taking account of the employee's exposure to opportunities for and attempts at misuse for the purposes of money laundering and terrorist financing) and the resulting responsibilities, duties and the level and frequency of training pertaining thereto. In determining the appropriate frequency of training, the financial institution observes the provisions of Article 20(3) of the Act (at least once per calendar year on a regular basis and always before an employee is assigned work in which he performs ad hoc tasks under the Act). The training plan, or its basic principles, should form a part of the Programme and should determine the basic outline, periodicity and content of employees training. Each employee concerned who performs tasks under the Act must be familiarised with the applicable Programme governing procedures in assessing customers and their financial operations, and concurrently the financial institution is required to ensure that each employee has permanent access to this Programme.

(9) Training of the financial institution's employees is focused in particular on familiarisation with the Programme and knowledge arising from the NO's activity, from the activity of other financial institutions, as well as available knowledge arising from the activity of the FIU, or the NBS.

(10) Specialised training that the employees of a financial institution should complete before they process customers' instructions for the execution of financial operations should give them the necessary knowledge for ascertaining and verifying a customer's identity upon the creation of a business relationship and in the provision of products and services and execution of transactions. Through participation in training events (seminars, educational stays) the employees acquire the necessary skills enabling them to know the expected type of a customer's commercial activities from their related financial operations, and, therefore, also the necessary knowledge and capability to identify facts outside the customer's expected behaviour, and specific manifestations of their UTs.

(11) A financial institution should repeat and supplement training with new knowledge, where necessary, also more frequently than in a 12-month cycle, so as to ensure that the relevant employees are able to continuously perform their duties and exercise their powers. A financial institution ensures that records are drawn on employees training conducted, containing the date at which the respective employees participated in the training, the content and form of the training, and, where relevant, an evaluation of the test completed, as well as the employees' signatures or other electronic confirmation. In addition to this, it is necessary to obtain from the respective employees a written or electronic confirmation that they have been familiarised with the Programme and related regulations governing AML/CFT procedures. Forms of training (classic lecture, electronic, or other) should be regularly alternated, eventually suitably combined. It is recommended to include elements of interactivity into the training process, such as providing online feedback to an employee during training.

(12) A financial institution must have a process of evaluating test results as well as follow-up procedure in the event of failing a test. In the event of failing a test this means setting a new date for retesting which cannot be carried out less than 3 days after failing the original test and at this time, such an employee may not be assigned a position responsible for AML field.

Article 8
Information system

(1) A systematic approach to the financial institution's risk management and ensuring AML/CFT requires mainly 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, including its statutory body, the NO, the deputy NO, the compliance and internal audit staff, and other relevant employees. In broad terms this means a system of acquiring, processing, evaluating, transferring and also using information relating to this field. This includes flows of AML/CFT information in the processes of the financial institution's individual activities and types of transactions performed. For effective prevention it is essential to ensure that it is regularly updated, with emphasis on the timely introduction of new types of transactions (which, prior to their inclusion in the existing range of activities and services, are assessed by the NO also in terms of the risk of their misuse for the purposes of money laundering and terrorist financing) in the information systems.

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

(3) The financial institution is required to ensure information flows mainly for:
(a) the transmission of information to employees on basic AML/CFT principles, procedures, duties and related powers required for performance of tasks in the given area;
(b) making the Programme and other relevant internal regulations available to all employees;
(c) the transmission of necessary information between the Responsible Person and NO;
(d) the transmission of information between employees and the NO and vice versa, including the internal reporting of UTs;
(e) the record-keeping, i.e. the recording, processing and updating of information on customers and the recording and monitoring of customers' transactions;
(f) communicating to the statutory body or Responsible Person the results of control performed by the NO and internal control and internal audit unit, as well as informing employees of these results;
(g) the transfer of information between the NO and FIU, including the reporting of UTs and provision of other necessary information and source documentation to the FIU, as well as the provision of feedback from the FIU to the financial institution;
(h) searching for unusual transactions in the financial institution's relevant information systems that contain information on customers and their operations.

(4) The form, content and rules of information flows should be set by the financial institution depending on its size, focus, scope and the complexity of its activities and on the types of transactions and services offered, as well as on the characteristics of its customers and their transactions. The information system(s) shall conform to the specific conditions of the financial institution and, from the technical aspect, have parameters so that the financial institution is capable of fulfilling the duties arising to it under the Act (in particular Article 21(2) of the Act) as an obliged entity.

(5) An essential component of a financial institution's information system is an electronic information system (hereinafter referred to as an "EIS") that complies with statutory requirements, with the aim of ensuring sufficient quality of AML/CFT prevention. It is a system recording and processing data on customers and their financial operations must take account of the requirements provided for in Article 7(e) of the Act:

(a) in the case of a natural-person customer, the EIS must contain the following information: a customer's full name, personal identification number or date of birth if personal identification number has not been assigned, permanent address or any other address, citizenship, type and number of identity document and account number;
(b) in the case of a natural-person entrepreneur, the same applies as under point (a) together with their place of business address, registration number, if assigned, as well as the designation of the official register or other official record in which this entrepreneur is registered, and the number of their entry in this register or record;
(c) in the case of a legal-person customer, the EIS must contain ascertaining of the following information: business name, registered office address, registration number, designation of the official register or other official record in which this legal person is registered and the number of their entry in this register or record, and identification data of a natural person authorised to act on behalf of the legal person, as under point (a).

(6) The EIS at the same time contains information or records on the method for identification and verification of the customer and information on the purpose and nature of the customer's business relationship which is given by the type of transaction pursuant to Article 9(h) of the Act, whereas the nature of the business relationship is primarily predetermined by the actual service used by the customer. The EIS and the manner of using it should make it possible to identify UTs performed by customers, and, as relevant, monitor also their course or development, as well as the connections between the financial operations of a certain customer and, where possible, also the UTs of different customers.

(7) A special part of information recorded and monitored by the EIS consists in data on politically exposed persons (Article 6 of the Act) and on shell banks (Article 9(c)) and Article 24(1) of the Act), which the respective employees received in performing their work tasks. Other situations in which the financial institution may use the EIS in providing information arise from Article 18(8) of the Act.

(8) The EIS should enable the financial institution to immediately provide the FIU, upon request, information as to whether it has or has had a business relationship with a specified person in the past five years, as well as on the nature of that business relationship (Article 21(1) of the Act).

(9) The EIS should also be capable of providing in a timely manner and sufficient scope data to the FIU, NBS as the supervisory authority and law enforcement authorities in cases specified by law, and last but not least, the EIS should also satisfy requirements for the purposes of control for the financial institution's own needs and for the needs of the FIU (Article 30 of the Act) as well as for statistical purposes.

Article 9
Customer identification and customer acceptance, customer risk profile; basic, simplified, and enhanced customer due diligence and compliance by third parties

(1) The basic obligations of a financial institution in these areas are laid down in particular in the provisions of Articles 7, 8 and 10 to 13 of the Act, and in separate regulations (Article 73 and 73a of AoSIS, Article 54a of AoOAPS, Article 28a of AoSPS, Article 55 of AoCI).

(2) A financial institution performs all elements of basic customer due diligence (natural person and legal person) under Article 10(1) of the Act always in situations referred to in paragraph

2 of that provision of the Act, relating to the activities of a financial institution (Article 10(2)(a) to (d)). This means that a financial institution performs the basic customer due diligence in relation to customer:

(a) in concluding a business relationship;
(b) in performing an occasional transaction worth at least EUR 15,000 outside a business relationship and in the event of an occasional cash transaction worth at least EUR 10,000 outside a business relationship, irrespective of whether the transaction is executed at once or sequentially through transactions that are or can be interlinked;
(c) where there is a suspicion that a customer is preparing or performing an unusual transaction, irrespective of the value of the transaction;
(d) if there are doubts about the correctness or completeness of data obtained previously, which is necessary for performing the customer due diligence.

(3) The basic customer due diligence of a financial institution in relation to customer includes:

(a) customer identification and verification of the customer's identity;
(b) identification of the beneficial owner and adoption of appropriate measures for verification of their identity, including measures to determine the ownership and management structure of a customer who is a legal entity or an asset pool; when identifying the beneficial owner, the obliged entity must not rely exclusively on data from the register of legal entities, entrepreneurs, and public sector entities;
(c) acquiring information on the purpose and intended nature of the transaction or business relationship;
(d) ascertaining whether the customer or their beneficial owner is a politically exposed or a sanctioned person;
(e) depending on the ML/TF risk, ascertaining the origin of funds or assets used in a transaction or business relationship;
(f) determining whether the customer is acting on their own behalf;
(g) continuous monitoring of the business relationship, including scrutiny of specific transactions executed during the business relationship in order to determine whether such transactions are consistent with what the obliged entity knows about the customer, including the customer's business profile and potential risk profile and ensuring that the customer's documentation, data and other information available to the obliged entity are kept up to date.

(4) A financial institution always identifies and verifies identification if the transaction value is at least EUR 1,000.

One of the fundamental obligations of a financial institution within the performance of a basic customer due diligence within the meaning of Article 10a(1) of the Act is the identification of the beneficial owner (Article 6a of the Act) and subsequent registration of identification data of the beneficial owner to the extent specified in Article 7(1)(a) of the Act. According to Article 10(7) of the Act it is necessary that the financial institution in the situations referred to in Article 10(2) of the Act ascertains whether the customer acts on his own behalf. In accordance with the provision of Article 73(5) of AoSIS (by analogy Article 55(3) of AoCI), the financial institution is required to perform this ascertaining even where this concerns a transaction at least in the amount of EUR 15,000 (i.e. not only an "occasional" transaction as implied by the Act) and a cash transaction worth at least EUR 10,000.

(5) The process of ascertaining and, to an appropriate extent, also taking measures to verify identification of the beneficial owner and registration of their identification data is governed primarily by the provisions of Article 6a, Article 8, Article 9, Article 10 and Article 10a of the Act. This means that it is always necessary to ascertain the beneficial owner, also in the case of legal

persons, whereas the legal form of a company (e.g. joint-stock company with bearer shares or a trust) may not obstruct the detection of the beneficial owner. Verification of information acquired on the beneficiary in accordance with the Act is to be performed to an appropriate extent, e.g. by requesting a written declaration on the beneficiary and subsequent verification of this information from available sources. Where the customer's risk profile so allows, the financial institution, in applying basic customer due diligence, may determine the beneficiary based on information from available sources, without the need to contact the customer or verify this information with them. However, during supervision, the obliged entity is required to demonstrate that the extent of performed customer due diligence is commensurate with the identified level of ML/TF risk (e.g. by monitoring or other demonstrable form).

In this regard it is necessary to respect the Guideline of the FIU as published on the website (http://www.minv.sk/swift_data/source/policia/finpol/PEPS-usmernenie-20052011.pdf) (first part of the Guideline).

For illustrating possible situations in ascertaining the customer's beneficial owner in the case of legal persons there is given an overview of practical procedures used in EU Member States, which are listed in the material drawn up and published in April 2012 in the Anti-Money Laundering Committee – AMLC) operating in the Joint Committee of European Supervisory Authorities, available on the website (http://www.esma.europa.eu/system/files/jc_2011_096.pdf).

(6) Where the beneficial owner is identified as a senior manager, the financial institution should take reasoned measures to verify the identity of a natural person holding a position in senior management and at the same time, it should register such records on taken measures taken as well as possible problems encountered during such verification process.

(7) The importance of the provisions of Article 10(1)(a) to (c) and Article 7 of the Act is highlighted in the provisions of Article 15 and Article 24(2) of the Act, which impose on the financial institution the duty to refuse new customers, terminate an existing business relationship with customers, or refuse to perform a specific business operation in the case where it is not possible to perform basic customer due diligence for reasons on the part of the customer pursuant to Article 10(1)(a) to e) of the Act. A comparable duty arises also under Article 73(3) of AoSIS. Under Article 17(1), a financial institution is required to promptly report such cases to the FIU.

In this context it is necessary to respect the FIU's instruction published on the website (http://www.minv.sk/swift_data/source/policia/finpol/usmernenie_paragraf_15.pdf).

(8) In performing activities under this Act, a financial institution is required to identify, assess, evaluate and update the ML/TF risk by type of transactions and business relations, taking into account own risk factors and risk factors as set out in Annex 1 of this Methodological Guideline. The obliged entity must determine the risk factors primarily based on the customer type, the purpose, regularity and duration of its business relationships or occasional transactions outside of these business relationships, the product type, the value and execution method of transactions, and the riskiness of countries or geographic areas related to its business relationships or transactions.

(9) When categorising customers to a certain risk category, a financial institution takes into account the information on the risk factors as set out in Annex 1 of this Methodological Guideline, in particular:
(a) sufficient information about the nature of customer's expected transactions;
(b) foreseeable and anticipated scheme of transactions to be performed by the customer.

(10) In the case of new customers, the customer acceptance process should include basic customer due diligence, as well as the customer's categorisation into a certain risk group,

accompanied by thorough application of the KYC principle, meaning the acquisition of sufficient information on the nature of the customer's expected transactions and any foreseeable scheme of operations to be performed by the customer. Based on this, it is possible to create the customer's risk profile. The main factors in the creation of the customer's risk profile include particularly the criteria as set out in Annex 2 as well the purpose pursued by the customer when entering into a business relationship, geographical area of the customer's business activities, the nature of business activities, the source of capital (funds), the source of funds (wealth), the frequency and scope of the customer's activities, the type and complexity of its business relationships.

(11) In applying basic customer due diligence, a financial institution may not enter a business relationship with a customer without reliably ascertaining all relevant circumstances concerning the customer (including ascertaining the beneficial owner and taking appropriate measures for verifying this information), as well as ascertaining the expected nature of trading, business or other activity anticipated by the customer. The AML employees must know their customers and their usual commercial, business or other activity. Based on the information acquired, employees of the financial institution and their direct superiors are then able, during the existence of the financial institution's business relationship with the customer, to assess each instruction of the customer for handling funds on the customer's account against the expected behaviour of that customer. In so doing they take account of circumstances that may indicate a change in the nature of the customer's business or a change in its usual activity and verify appropriately these facts.

(12) The financial institution continuously updates the customer's risk profile according to the risk group to which the customer is assigned; on the basis of which it requires from the customer to update the data that the customer originally provided, or has previously adjusted, and this in appropriate time intervals and depending on changes concerning the customer's person, or their commercial or other activities with which the customer's financial operations are connected. Updating may be performed also by way of requesting the customer to complete the relevant form, for example once a year, unless more frequent updating is necessary, or by agreeing a contractual condition with the customer on the duty to report relevant changes.

(13) By means of categorising customers according to their risk profile the financial institution can then in practice apply Article 10(1)(g) of the Act, namely ongoing monitoring of the business relationship, which leads to recognition and subsequent reporting of unusual transactions. In connection with the risk categorisation of customers, the financial institution should consider also Article 10(1)(g) and Article 10(6) of the Act, which establish the duty to continuously update the customer's risk profile based on a permanent monitoring of the business relationship. The appropriate frequency for updating depends on the financial institution's assessment and decision; in each case this duty should be included in its Programme of own activity.

(14) Subject to Article 9(d) of the Act, the customer means the person that is a party to the obligation relationship associated with the obliged entity's business activity. The portfolio management being one of the provided investment services of the investment firm within the meaning of Article 6(1)(d) of the AoSIS, it is necessary that the investment firm takes all measures in managing the portfolio of the customer's financial instruments for identification of the customer and fulfilment of other obligations arising from its relationship with the customer (customer due diligence, KYC, or reporting of UT) also in respect of persons that are a counterparty in a transaction. This does not apply to transactions carried out on a regulated market or in a multilateral trading system or organized trading system within anonymous trading.

In connection with the consideration of risk in assessing a financial institution's customers, it is appropriate to use materials prepared by experts of the FATF and the MONEYVAL Committee

of the Council of Europe, regularly published (updated three times a year) conclusions from the ongoing monitoring of countries that have significant shortcomings in the enforcement of AML/CFT measures, e.g.:
(a) the FATF Public Statement (http://www.fatf-gafi.org/topics/high-riskandnon cooperativejurisdictions/documents/fatfpublicstatement-19october2012.html); i.e. the "black list";
(b) improving global AML/CFT compliance on-going process available on the website (http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/documents/improvingglobalamlcftcomplianceon-goingprocess-19october2012.html); i.e. the "grey list";
(c) valid conclusions from FATF monitoring available on the website of the FIU (http://www.minv.sk/?vyhlasenia-fatf);
(d) the formal publication on a Member State, confirming that the country does not comply with the basic reference documents for appropriate prevention of money laundering and terrorist financing, available on the website (http://www.coe.int/t/dghl/monitoring/moneyval/);
(e) currently valid conclusions from monitoring are published also on the website of the FIU (http://www.minv.sk/?moneyval-vyhlasenia);
(f) detailed evaluation reports on each Member State and its system of prevention and repression in the field of money laundering and terrorist financing (in the form of a "Mutual Evaluation Report"), available in English on the website (http://www.fatf-gafi.org/topics/mutualevaluations/ and http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/Evaluation_reports_en.asp);
(g) the list of equivalent third countries, which was created on the basis of agreement of the EU Member States in the European Commission committee ("CPML/TF" – Committee on Prevention of Money Laundering and Terrorist Financing), available on the Committee's website (http://ec.europa.eu/internal_market/company/docs/financial-crime/3rd-country-equivalence-list_en.pdf) as well as on the website of the FIU (http://www.minv.sk/?ekvivalent).

(15) The Act, in accordance with the implemented EU directives, defines only the basic situations that pose an increased risk of money laundering and terrorist financing. However, the financial institution must apply a more stringent procedure for the identification and verification of facts ascertained and subsequent monitoring of the business relationship with a customer also in other situations, according to the customer's risk profile or according to the degree of risk inherent in the service or type of transaction provided to the customer (legal persons not entered in the commercial register, e.g. political parties, legal persons in the form of joint-stock companies with bearer shares, joint accounts, accounts connected with custodianship, etc.).

(16) Enforcement and compliance of all these procedures and rules (identification, verification, KYC) provides, besides the recognition of unusual transactions and minimisation of the risk of money laundering and terrorist financing, also protection against fraud.

(17) Where the customer poses a high risk, this requires more detailed assessment of the customer, the customer's behaviour and orders given by the customer for financial operations. It is then necessary to take measures to eliminate the risk to an acceptable level.

The financial institution exercises enhanced customer due diligence in situations that, with regard to their nature, may pose a high risk of money laundering or terrorist financing. It also pays particular attention to selected groups of subjects, in addition to the already mentioned politically exposed persons (Article 6, Article 10 and Article 12 of the Act), particularly asset pools (Article 25(2) of the Act) and shell banks (Article 24(1) of the Act).

In the case of identifying politically exposed persons, financial institutions are recommended, in accordance with the new FATF international standards published in February 2012 on the website (http://www.fatf-gafi.org/topics/fatfrecommendations/documents/fatfrecommendations2012.html) to exercise

enhanced customer due diligence not just to the sphere of persons referred to in Article 6(1) of the Act, but also to persons with permanent residence in the Slovak Republic. In the process of the identification and verification of politically exposed persons it is recommended to use the existing commercial databases of high-risk customers, e.g.: World-Check database of high risk individuals and companies; website (http://www.world-check.com/). In monitoring existing customers it is essential to focus also on the ongoing monitoring and verification as to whether the customer has become a politically exposed person; in such a case, to continue the business relationship, the consent of a manager must be required, meaning an employee one or more management levels higher than the employee who normally concludes such business relations within the meaning of the organizational structure of the financial institution, under which the responsibility for the area is clearly defined. Where a politically exposed person owns or works in the managing structure of a customer – legal person, or is a beneficiary, in such a case this constitutes a situation requiring the application of enhanced customer due diligence towards the customer – legal person.

In this regard it is necessary to respect the guideline of the FIU (in particular its second part) as published on the website (http://www.minv.sk/swift_data/source/policia/finpol/PEPS-usmernenie-20052011.pdf).

A financial institution applies enhanced customer due diligence in relation to customer also if it is preparing to establish a new business relationship or payment account without the customer being physically present.

(18) The Act in its Article 13 allows the use of customer due diligence already performed by a different credit or financial institution in applying customer due diligence procedures, i.e. performance by third parties, other than for the ongoing monitoring of a business relationship under Article 10(1)(g) of the Act. This means that, as regards compliance with the conditions referred to in this provision, it is possible to rely on already-performed identification and verification of the customer and beneficial owner and to receive or provide data on this identification and verification from/to a credit or financial institution (in the scope under Article 5(1)(b) points 1 to 10 of the Act) operating within the EEA (i.e. a third party), including those institutions operating in the territory of the Slovak Republic.

Exchange offices and payment institutions are outside the sphere of obliged entities from which it is possible to accept identification and verification of a customer and beneficial owner.

Responsibility for the fact that information thus acquired meet the requirements for exercising customer due diligence under the provisions of the Act, nonetheless remains with the financial institution that decided to rely on the third-party performance approach. In such cases, in accordance with the practice in EEA member countries, it is not necessary to specifically require the customer's consent to the provision of data to a third party.

Under Article 13(4) the Act considers outsourcing to be an activity performed for a financial institution on the basis of its rules and regulations, and therefore such situations are not deemed to constitute third-party compliance.

(19) A financial institution can exploit the possibility of applying a less demanding procedure in customer identification, i.e. simplified customer due diligence (Article 11 of the Act). The use of simplified customer due diligence in no way represents an exemption from the duty to monitor the business relationship on an ongoing basis (Article 10(1)(g) of the Act), or from other duties defined by the Act, so that it is possible to comply with the provisions of Article 14 and Article 17 of the Act, as well as others, including the duties to process and archive data according to the provisions of Article 19 and Article 21 of the Act. Simplified customer due diligence of the obliged entity means the identification of the customer, where no verification of such identification is required. A more detailed procedure for applying simplified customer due diligence in relation to customers is set out in Annex 1 of this Methodological Guideline.

In connection with the use of simplified customer due diligence there comes into consideration also the possibility to use a list of equivalent third countries, as created by agreement of the EU Member States, and published in English on the CPML/TF website, and on the FIU website. The fact that a country is included in the list, however, does not preclude that a customer from the country may be included in a higher risk category. Indeed, it is always necessary to consistently fulfil duties under the provisions of Article 10(1)(d), Article 10(4) and (6) of the Act.

Article 10
Detection, reporting and delaying of UTs

(1) As part of performance of its AML activity, the financial institution makes a list of most common recurring UTs or of the severest forms of UTs which should be part of the Programme of own activity. For identifying unusual transactions, it is crucial to apply the provisions of Articles 2 to 4, Articles 10 to 12 and Articles 14 and 20 of the Act.

Under Article 14(1) of the Act a financial institution is required to assess whether an intended or ongoing transaction is unusual. Under Article 20(1) and (2)(d) of the Act a financial institution must regulate this part of the procedures in its Programme.

Duties referred to in Article 14(1) and (2)(a) and (b) of the Act must be fulfilled demonstrably so that the financial institution can, in accordance with Article 30(3), in the case of an inspection, provide information and written documents on the fulfilment of these duties.

Article 14(3) of the Act also emphasises the duty to draw up records on transactions under Article 14(2)(a) of the Act (i.e. internal reporting of UTs), which must also contain information justifying the result of the assessment of a product, service or transaction) and which must be archived within the statutory period (Article 19 of the Act).

(2) An unusual transaction is a legal act or other act that indicates that its execution may lead to money laundering or terrorist financing (Article 4 of the Act). Article 4(2) of the Act gives a demonstrative calculation of a UT. More detailed forms and methods of money laundering and terrorist financing and indicators for detecting unusualness are set out in Annex 2 of this Methodological Guideline.

There are several signs (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 the financial institution is required to assess, identify, evaluate and concurrently apply the KYC principle (the Act does not define any KYC principles, though where an obliged entity applies them in practice, it is necessary to thus define them in the Programme).

Only by such action can it competently assess whether a customer's intended or ongoing transaction is unusual or not. The Act in Article 4 does not stipulate any criteria, e.g. in the form of threshold amounts of funds that would lead to the automatic finding in the case of a certain type of financial operation that it undoubtedly constitutes an unusual transaction. The decisive element for assessing the 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 the financial institution is required to determine for itself, depending on the subject and scope of its activity and the type and extent of products, services and transactions performed for customers, in the framework of drawing up an overview of the forms of UTs (Article 20(2)(a) of the Act). Based on practical experience of supervisions exercised by the competent bodies, the following transactions can be considered a UT within the assessment of all identifiers of unusualness: execution of transaction (purchase – sale of securities) by an agent who is an identical person in the case of both the transferee of securities and the original holder of securities, transfer of shares of a company that was declared bankrupt, with the transferor and the transferee being an identical person (member of the board of directors), arrangement of deals with securities from a risk country, transfer of funds for arrangement of deals from an account other than that specified by the customer without apparent

reason or explanation, the customer having permanent residence in an offshore country (tax heaven), as well as an UT within the specific regulation of the old-age and supplementary pension scheme – it can be the payment of a contribution to the old-age or supplementary pension saving scheme which deviates from the usual payments by the customer as for the amount or unusual frequency.

(3) The conditions for the proper application of the KYC principle derive from the duties of the financial institution and customer, as set out in Act (Articles 10 to 12). The crucial provisions are those of Article 10(1), (4) and (5) and Article 11(3) of the Act.

Such procedure enables a financial institution to satisfy itself adequately as to the actual identity of each customer and 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, subsequent determining the degree of customer due diligence pursuant to Article 10(4) of the Act and accepting a customer. A financial institution then, depending on the result, applies procedures in the framework of basic customer due diligence under Article 10 of the Act or simplified customer due diligence under Article 11 of the Act or enhanced customer due diligence under Article 12 of the Act.

(4) A financial institution is required, in applying each type of customer due diligence, to assess whether an intended or ongoing transaction is unusual (Article 14(1) of the 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 on them, i.e. internal reporting of an UT (Article 14(3) of the Act) in accordance with paragraph (10) the last sentence of this Article.

(5) A financial institution performs skilled assessment of intended and ongoing transactions at various time intervals and at various levels. The assessment process takes place:
(a) on the frontline, where the financial institution's employees are in contact with an existing or potential customer;
(b) in the framework of ongoing monitoring of an existing business relationship;
(c) in the framework of subsequent (retrospective) assessment of a customer's transactions.

(a) Assessment of transactions at initial contact with the customer before and during execution of a transaction

In concluding a business relationship (Article 10(2)(a) of the Act or occasional transaction (Article 10(2)(b) and (c) of the Act), the assessment of such customer's transaction is performed by employees of the financial institution who, in fulfilling their duties, are in contact with the customer, thus those employees who receive or process customers' instructions for execution of their transactions or financial operations, or superiors of such employees. The assessment of a transaction by an employee of the financial institution is thus performed largely at the place of executing the transaction and prior to its conduct, or at an attempt to execute a transaction so that an unusual transaction can be postponed and promptly reported.

Every relevant employee is required to have the Programme permanently available, either in paper or electronic form and is required to learn it and proceed according to it. An employee of a financial institution follows in this stage primarily Article 10(1) as well as Article 11(3) of the Act, which enables the employee to ascertain to an appropriate degree the real identity of the customer and to know the purpose and planned nature of the business activities that the customer will probably perform. This procedure is also the starting point for the financial institution in accepting a customer, determining the customer's risk profile and then determining the degree of customer due diligence pursuant to Article 10(4) of the Act.

A crucial element for assessing customers' transactions is the appropriate application of the

KYC principle and its procedures and skilled identification of signs of unusualness. This procedure enables the employee to assess customer's intended or ongoing transactions by comparing them against an overview of types of unusual transactions (Article 20(2)(a) of the Act), as well as against forms referred to in Article 4(2) of the Act and to detect those that are unusual in relation to the customers and their otherwise usual transactions.

If an employee assesses an intended or ongoing transaction to be unusual, they make a written record on this transaction in accordance with Article 14(3) of the Act and promptly notify this finding to the Nominated Officer (hereinafter the "notification of unusual transaction").

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

The competent employees of the financial institution assess the customer's transactions also in the framework of ongoing monitoring of the business relationship.

The assessment of intended or ongoing transactions in the framework of ongoing monitoring of the business relationship is specific in that the business relationship has already started and continues (Article 10(2)(a) of the Act). The customer may also be known to the financial institution where the customer has already executed several occasional transactions (Article 10(2)(b) or (c) of the Act). Therefore, this is not the first contact with the customer and the financial institution may take account of the customer's existing risk profile and history of transactions performed by the customer.

The procedure according to Article 10(1)(d) of the Act, including verification of the completeness and validity of identification data and information under Article 10(6) of the Act and the customer's duty under Article 10(5) of the Act form the basis for ongoing monitoring of the business relationship. This type of monitoring requires the creation of customer risk profiles and their classification with regard to the possible risk of money laundering and terrorist financing under Article 10(4) of the Act. In creating customer risk profiles, a financial institution makes use of the overview of the risk factors as set out in Annex 1 of this Methodological Guideline. In the event of proving an UT in the framework of monitoring of the business relationship, a financial institution updates the customer's risk profile under Article 9(11) of this Methodological Guideline and reassesses the customer's risk category.

Ongoing monitoring of the business relationship requires the use of an appropriate EIS that enables the financial institution, in accordance with risk-based prevention, to create financial or other criteria or limits as indicators of unusualness in customer' transactions 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 criteria or limits defined by the institution for this purpose must be regularly verified so that it is possible to determine their adequacy in regard to the identified levels of risk. The financial institution is required also to regularly review the adequacy of the existing system and individual processes of protection and prevention.

For assessing transactions, importance is be given, in the framework of ongoing monitoring of the business relationship, to intended or ongoing transactions of a customer that do not correspond to the customer's known or expected activity or that correspond to types of unusual transactions as set out to in the Act or as specified in more detail in the Programme. Such transactions of a customer form subject of assessment (Article 14(2) of the Act) and it is necessary to make a written record of them containing the rationale behind the results of the assessment (Article 14(3) of the Act), whilst these records must be archived in accordance with the period referred to in Article 19 of the Act.

The NO may, based on results from the assessment of the various circumstances of a transaction and with regard to the overview of types of unusual transactions, reach the conclusion that in the given case it does not constitute an unusual transaction. If the conclusion cannot be reached solely based on information on the customer that the financial institution already has available, it may, according to circumstances, request other necessary information and documents

from the customer, pursuant to Article 10(5) of the Act.

In cases where the NO is unable, even through this procedure, to identify the reason for the customer's transactions that do not correspond to the customer's risk profile or to its known or expected activities, 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 (Article 17 of the Act).

The assessment of transactions in the framework of ongoing monitoring of the business relationship is performed, depending on the transaction, by employees as well as the NO.

(c) Assessment of transactions in the framework of subsequent 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 by a 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.

(6) The recommended procedure in the processing and handling of internal notifications of unusual transactions and unusual transaction reports is as follows:
(a) all internal notifications of UTs sent by competent employees to the NO must be documented according to Article 14(3) of the Act and must be available for the purposes of inspection according to Article 29 of the Act;
(b) the sending of internal notifications and reports to the NO may not be subject to the prior consent of any person (e.g. superior);
(c) the NO registers and archives notifications on internal notifications of unusual transactions, including the position, first name, last name, workplace or unit of the financial institution and all data on the given customer and transaction in accordance with Article 19 of the Act;
(d) the NO, as well as employees of the financial institution, including its managers (members of the statutory body) involved in assessing transactions under Article 14 of the Act are required to maintain confidentiality on the notified and reported UTs and on measures taken by the FIU, including the fulfilment of duties under the provisions of Article 17(5) and Article 21(1) of the Act; whilst the financial institution may not, however, cite toward Národná banka Slovenska the duty to maintain confidentiality in connection with the performance of supervision and inspection under Article 29 of the Act (Article 18(5) of the Act). Provided that information given is used exclusively for the purposes of preventing money laundering or terrorist financing, the duty of confidentiality does not apply to the provision of information between credit or financial institutions under the conditions set out in Article 18(8)(a) and (c) of the Act;
(e) the financial institution is required to draw up a procedure covering the period from the moment of detecting an UT through to prompt reporting of the UT, including the procedure and responsibility of employees who assess the transaction;
(f) the NO, after receiving an internal notification of an UT, demonstrably confirms its receipt to the employee who sent the notification. The confirmation should contain an instruction on the duty to maintain confidentiality under the Act. Where the financial institution has an electronic system of gathering internal reports that enables the competent employee to monitor the status or receipt of a submitted internal report of an UT by the NO, or by the Prevention Unit, the procedure under the first sentence is not needed;
(g) The internal notification of an UT, or the conduct of a customer, the transaction and/or financial operation that the notification concerns is the subject of an assessment by the NO, who may, on the basis of results from further assessment of the various circumstances of the transaction, and with regard to the overview of types of unusual transactions, decide whether it does or does not constitute an UT. This internal notification contains information on the economic or lawful purpose of the transactions and, in the case that the transaction is usual, also sufficient reasoning regarding

its usual nature. Otherwise the process of such assessment cannot be considered trustworthy and objective. If the decision cannot be reached solely based on information on the customer that the financial institution already has available, it may, according to circumstances, request other necessary information and documents from the customer, pursuant to Article 10(5) of the Act. Where the NO reaches the justified conclusion that in the case of an internally notified UT it does not actually constitute an UT, the NO is required to document this decision in writing and to archive all related data, written documentation and electronic documentation in accordance with the period referred to in Article 19 of the Act,

(h) In cases where the NO cannot even through this procedure reach the conclusion that it is not an UT, it is enough that the transaction and/or financial operation indicates that its execution may constitute money laundering or terrorist financing, and the NO is required to report the unusual transaction to the FIU.

The financial institution is required to promptly report the UT or an attempt to execute the UT to the FIU, i.e. at the earliest opportunity (Article 17(1) of the Act). It is necessary to take into consideration the particular circumstances of the situation in which the finding of the UT is made, whilst an UT must be reported as soon as possible. A decision of the NO to report an unusual transaction must not be subject to the prior consent or approval of any other person. A report of an UT contains at least the data specified in the Act. The reference number of each report of an UT should take the form: serial number / year / character code of the financial institution, e.g. 1/2009/SUBA.

An unusual transaction may be reported in writing, electronically or by telephone (in this case it is necessary to report the unusual transaction also in person, in writing or by e-mail within 3 days). The specimen form for reporting an unusual transaction, issued by the FIU, is given on the website (https://www.minv.sk/?vzory-hlaseni-o-noo).

An unusual transaction report may be supplemented at the financial institution's own initiative within 30 days. After this period, it is necessary to additionally report information and documentation acquired as another UT. In this subsequent unusual transaction, the financial institution states the unusual transaction to which the additionally acquired information and documentation relate. In connection with the reporting of unusual transactions and sending of further supplementary information, as well as the overall communication and exchange of information with the FIU, it is recommended in the interest of compatibility and streamlining of the procedure in the reporting process, as well as in the interest of streamlining control processes, that financial institutions communicate with the FIU by electronic means via the electronic registry, while complying with the conditions for protection of transmitted information and for clear identification and verification. Only in this way is it possible to avoid security risks connected with the reporting of UTs by post, fax and e-mail.

(7) The financial institutions are allowed, under defined justified conditions, to exchange information where this is related to the threat of money laundering or terrorist financing, and where it helps the obliged entities assess a customer's transactions more effectively as well as alert other obliged entities to identified risks. An exchange of information should not contain the full scope of the reported UT as a whole, if this is to violate bank secrecy or unauthorized disclosure of customer's personal data subject to confidentiality. The subject of the exchange should be the information obtained under the procedure laid down in Article 10(1) of the Act to such an extent as to be able to use the obtained information relating exclusively to the ML/TF risk. Information provided can pursuant to the Act be used exclusively for the purposes of preventing money laundering or terrorist financing.

(8) The financial institution delays an UT, i.e. the execution of a transaction (Article 9(h) of the Act) in accordance with the customer's instructions, until the time of its reporting to the FIU, whilst account is always taken of the operating and technical possibilities, as well as of 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. The financial institution is required under the Act to delay an UT in the following cases:
(a) if execution of the unusual transaction poses the risk that there may be frustrated or substantially impeded the seizure of proceeds from crime or seizure of funds intended for financing terrorism, at its own discretion, whilst the financial institution is required to immediately inform the FIU;
(b) upon written request of the FIU.

(9) The financial institution will not delay an UT if it is unable to do so for operating or technical reasons (it immediately notifies 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.

(10) The period of delaying an operation assessed as unusual is at most 120 hours (Article 16 of the Act); therefore, if during this period the FIU notifies the financial institution that it has forwarded the case to the law enforcement authority, the financial institution is required to extend the period of delaying, though no more than by a further 72 hours. Therefore, the total duration of delaying an unusual transaction is no more than 192 hours. If during the period 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 referred to as the "Code of Criminal Procedure"), the financial institution executes the delayed operation following the expiry of the set period. Prior to the expiry of the period of delaying, the financial institution may execute the operation only in the case that the FIU notifies it in writing that from the aspect of processing the unusual transaction, its further delay is not necessary. Saturday and bank holidays are not counted in the period of delaying an UT.

The period of delaying an operation pursuant to Article 16 of the Act is deemed to begin at the moment when the customer expresses the intention (will) to use the funds on their account. Where the financial institution presumes that the customer will express an intention to execute an unusual transaction (use funds) in the future, it is required to take personnel, organisational and technical measures so that in the case that the customer does give such instruction, it is not executed and thereby any potential delay of the unusual transaction is not frustrated.

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, the reason for delaying a transaction may not be the fact that the customer requested from the financial institution general information regarding an account (information on the account balance, etc.).

Article 11
Measures countering terrorist financing

Terrorism represents one of the most serious forms of breaching values such as human dignity, freedom, equality and solidarity and respect for human rights and fundamental freedoms on which the European Union is founded. It also represents one of the most serious attacks on the principle of democracy and the principle of the rule of law, which are common to Member States and on which the European Union is founded. The Act prohibits the financing of terrorism and requires financial institutions to pay attention to transactions that may be related to terrorist financing.

The International Sanctions Act defines an international sanction as a restriction, instruction or prohibition issued for the purpose of maintaining or restoring international peace and security, the protection of fundamental human rights and the fight against terrorism. At the same time it specifically defines international sanctions in the field of trade and non-financial services, in the field of financial services and financial markets, money transfers, the use of other means of

payment, the purchase and sale of securities and investment coupons, in the field of transport, posts, postal services and electronic communications, in the field of technical infrastructure, in the field of scientific and technical relations, in the field of cultural and sports contacts, in the field of restrictions on the exercise of property rights and in the field of travel and issuance of travel visas.

(1) In the framework of counter-terrorist financing measures, it is necessary that all financial institutions to which this Methodological Guideline applies focus on direction of the exit of funds which can be used for activities leading to terrorist financing. The measures should be focused on beneficial owners.

(2) Examples of UTs relating to terrorist financing can be identified as actions in the case of which there is a justified assumption that funds or assets are to be used or were used to finance terrorism, or there is a justified assumption that the beneficial owner is a person collecting or providing funds or assets to finance terrorism, or the action is executed from a country or into a country where terrorist organizations operate or are supported.

(3) Procedure of the financial institutions in fulfilling their counter-terrorist financing obligation in the form of reporting duty:
(a) in the framework of counter-terrorist financing in relation to customers, the financial institutions apply procedures analogous to those applied in AML, including the reporting of UTs connected with terrorist financing;
(b) financial institutions are required to report unusual transactions to the FIU promptly (Article 17(1) of Act) and the Act defines unusual transactions as, inter alia, a transaction in which there is a justified assumption that the customer or beneficial owner is a person against whom international sanctions have been imposed, or a person which may be in a relationship with that person, or as a transaction in which there is a reasonable assumption that the subject of it is or should be a thing or service that may relate to a thing or service against which sanctions are imposed under the International Sanctions Act.

(4) The financial institutions of all EU Member States are, based on the individual regulations and decisions of the EU, whose annexes contain lists of persons subject to sanctions (natural persons and legal persons), required to immediately freeze financial and economic resources of persons subject to sanctions from states listed in the annexes to the individual regulations and decisions of the EU. The 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 Common Foreign & Security Policy (in the framework of enforcing the Common Foreign & Security Policy) are listed on the website (https://eeas.europa.eu/topics/sanctions-policy_en.).
In this regard, the EU sanctions are listed on the website of the Ministry of Foreign Affairs of the Slovak Republic https://www.mzv.sk/zahranicna-politika/medzinarodne-sankcie, http://eeas.europa.eu/cfsp/sanctions/docs/measures_en.pdf).).
A consolidated list of sanctions is published on the website:
https://www.un.org/securitycouncil/sanctions/un-sc-consolidated-list

(5) The financial institutions in Slovakia are required to apply sanctions announced by EU regulations directly, as sanction measures concerning economic relations with third countries, for example freezing of financial assets and economic resources, are implemented by an EU regulation and are directly binding and applicable in the EU. Regulations have general application and are directly applicable in all Member States. As legally binding acts they take precedence over acts of the Slovak Republic, and they are also the subject of legal assessment by Slovak and European courts.

(6) Generally, three types of sanction measures are recognized:

(a) sanction resolutions of the UN Security Council

The UN Security Council Resolution against Terrorism is a document that provides the basis for criminalisation of incitement to terrorist acts and recruitment of persons for such acts. Resolutions call on states to adopt necessary and appropriate measures and, in accordance with their obligations arising under international law, prohibit by law the incitement to commit terrorist acts and to prevent such activity.

With regard to the above, sanctions are adopted through the transposition of sanction resolutions of the UN Security Council. This means that following the issuance of a UN Security Council resolution, it is necessary to implement the resolution in the shortest possible time in an EU regulation or in a common position of the EU.

An overview of comprehensive resolutions, sanction committees and UN policy against terrorism is published in English on the UN Security Council website (http://www.un.org/Docs/sc/).

(b) autonomous sanctions adopted by the EU

The EU Common Position 2001/931/CFSP as amended by Common Position 2008/586/CFSP published a list of persons subject to sanctions (natural persons and legal persons) associated with terrorism and against whom it is necessary to apply sanctions in the fight against terrorism. Persons listed in EU Common Position 2001/931/CFSP are broken down into external terrorists and internal terrorists (in this case persons marked with an "*", who are EU citizens or are domiciled in the EU, e.g. members of the Basque organisation ETA and extremist groups, in particular from Spain and Northern Ireland).

Financial sanctions are applied against the group of external terrorists under Article 3 of EU Common Position 2001/931/CFSP. Implementation of these sanctions is governed by EU Council Decision 2005/428/CFSP and Council Regulation No 2580/2001, which in practice means that, on the basis of directly applicable EU legislation, sanctions are binding for everybody in all EU Member States and are directly enforceable.

Financial sanctions are not applied against internal terrorists, since this is not permitted under the EU Treaty, which establishes a mandate for implementation of restrictive measures within the single market and financial services only towards third countries (Articles 60 and 301 of the EU Treaty, i.e. there is no mandate for imposing financial sanctions at the Community level against the EU's own citizens). Against internal terrorists, only so-called enhanced judicial and police cooperation apply at the EU level on the basis of Article 4 of the EU Common Position 2001/931/CFSNP and in accordance with Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences.

c) procedure in the case of persons against whom sanctions have been declared under a decree of the Government of the Slovak Republic

Persons included in the list of the EU Common Position 2008/586/CFSP, marked with an "*" are, however, terrorists and, on the basis of UN Security Council Resolution 1373/2001 on the suppression of terrorist financing, as well as on the basis of Article 2 of the EU Common Position 2001/930/CFSP, all countries have the duty to freeze economic and financial assets of all persons designated as terrorists or who provide assistance thereto, or who are in any way linked to terrorist structures.

The Slovak Republic declares international sanctions through a Government Decree, unless these result directly from the applicable law of the EU Act in accordance with Article 3 of the International Sanctions Act. Under Article 288 of the Consolidated Text of the EU Treaty, such an

act is a regulation with general application. It is binding in its entirety and is directly applicable in all EU Member States. In Slovak law, international sanctions are declared by Slovak Government Regulation No 397/2005 Coll. declaring international sanctions ensuring international peace and security, as amended by Government Regulation No 209/2006, No 484/2006, No 488/2007 and No 239/2008, 168/2009 and Decree No 442/2009 (hereinafter referred to as "Decree No 397/2005"). Decree No 397/2005 and relevant EU regulations laying down restrictive measures include a list of those persons subject to sanctions whose activity is confined to the territory of EU Member States, or who are EU citizens. Financial institutions are required to immediately freeze all financial and economic assets of persons subject to sanctions included in the list published in the annex to the SR Government Decree No 397/2005 or in the relevant EU regulations governing restrictive measures.

Based on the NRA conclusions it should be noted that financial institutions are cautiously reviewing transactions that could be linked to countries with terrorism risk and countries that also consistently comply with the EU and UN sanctioning regimes, even in low risk areas. However, attention should also be drawn to the increasingly new and sophisticated ways to raise funds, such as hostilities, terrorist acts or the payment of seemingly unrelated costs, and thereby encourage financial institutions to constantly increased attention and consistency in monitoring available resources and to adapt their procedures when verifying their customers.

In relation to the risk of terrorist financing, the FATF in its reports also warns about virtual currencies which offer a great opportunity for financial innovations, thus attracting the attention of different groups and thereby increasing the risk of terrorist financing.

Article 12
Archiving and storing of data and documentation

(1) The financial institution is entitled, for the purposes of performing customer due diligence (Article 10 to 12 of the Act) and for the purposes of detecting UTs (Article 14 of the Act) and without the consent and without informing the customer concerned, to ascertain, acquire, record, store, use and otherwise process a customer's personal data and other data, including the data and information obtained by technical means and procedures in identification of the customer in the event of their physical absence in the scope of the provisions of Article 10(1) and Article 12 of the Act.

(2) The financial institution is entitled to acquire the necessary personal data also by copying, scanning or by other recording of official documents on information media, as well as to process birth registration numbers and other information and documents without the customer's consent and in the scope set out in the mentioned provisions of the Act.

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

(4) Within the meaning of Article 19(1) and (2) of the Act, the financial institution is required to store for the period of five years:
(a) from the end of the contractual relationship with a customer, information and written documents acquired by way of the procedure under the provisions of Articles 10 to 12 and Article 14 of the Act,
(b) from the execution of a transaction, all data and written documents on the executed transaction.

(5) In view of the importance of information acquired by financial institution in fulfilling AML/CFT duties under Article 14(2)(a) of the Act, the financial institution is required to store the

written records referred to in paragraph 3 of that provision in the statutory period (five years from the written record being made).

(6) The financial institution is required to store this data and written documents also for longer than five years if the FIU requests it by way of a written request containing the period which may not, however, exceed other five years, scope of archiving data and written documents. This duty also applies to a financial institution that terminates its operation, up until the expiry of the period during which it is required to store these data and written documents.

(7) The financial institution's procedure in storing data and documentation, and records related to AML/CFT is governed by the financial institution's Programme, which should, in accordance with the Act, specify in more detail the following:
(a) the records that need to be archived (at least information on customer identification and records on the customer's transactions, including written records under Article 14(3) of the Act and information on identification of the beneficiary);
(b) the form of records (paper, electronic);
(c) the place, method and period for which records are to be archived, taking account of
1. the end of the contractual relationship with the customer;
2. the execution of a transaction with the customer; and
3. any written request of the FIU and the period specified (Article 19(3) of the Act).

(a) records that need to be stored/archived

1. records on customer due diligence performed
A financial institution stores the data and written documents of customer due diligence performed (basic, simplified, enhanced) acquired in accordance with the provisions of Articles 10, 11 and 12 of Act No 297/2008, like the identification and verification of a customer's identity, identification of the beneficial owner, information on the purpose and intended nature of a product, service or transaction, identification of politically exposed persons or persons subject to sanctions, ascertaining the origin of property and the source of funds depending on the AML/CFT risks.

2. records on customers' risk rating
Documents and information related to customers' assignment to risk groups must be stored. The financial institution records and stores any important information confirming circumstances justifying a customer's reassignment to a different risk category (and therefore a change of their risk profile) together with other information on the customer.

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

4. records on internal notifications of unusual transactions and unusual transaction reports
The financial institution is required to store all reports on the customer's unusual activities, namely internal notifications of UTs intended for the NO, as well as UT reports that the NO sent to the FIU. If the NO, after assessing the relevant information and knowledge concerning a customer's unusual

activity decided that it did not constitute an UT and did not report it to the FIU, the reasons for that decision must also be recorded and archived together with the records on the particular transaction.

5. records on implemented education and training

The financial institution stores the records on staff training, containing the date and content of the training and the confirmation that the respective employee attended the training and was familiarised with the financial institution's AML/CFT Programme, as well as related internal regulations of the financial institution.

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

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

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

The financial institution stored such information and documents also following the expiry of the statutory period for those customers and their financial operations in the case of which an investigation has been started from the side of law enforcement authorities, or a criminal prosecution begun, and for the purposes of investigation and criminal prosecution, on the basis of a written request by the FIU pursuant to Article 19(3) of the Act, in the scope and for the period stated in the request. Copies of documents in paper form must be made in such a way that the data is legible. Photography of the identified customer in their identity document must be of high enough quality to allow the verification of the customer's visual identity.

In this context it is necessary to respect the FIU's instruction published on the website (http://www.minv.sk/swift_data/source/policia/finpol/Par19ods-2-pism-b-usmernenie.pdf).

(8) Records prepared and stored by the financial institution must satisfy statutory requirements for record keeping on customer data and also enable:

(a) an independent party to evaluate the efficiency of compliance with basic principles, as well as the financial institution's AML/CFT procedures;

(b) reconstruction of the course of financial operations made by the financial institution for a customer;

(c) identification and location of each customer;

(d) identification of all internal notifications of unusual transactions and external unusual transaction reports;

(e) fulfilment within a reasonable time of statutory requests by the FIU, supervisory authority and law enforcement authorities concerning a customer and a financial operation.

Article 13
Securing the system and ensuring performance of internal control

The financial institution must have in place a reliably functioning system of control focused in part on the fulfilment of AML/CFT measures.

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

(a) the financial institution's supervisory board;

(b) members of the financial institution's statutory body;
(c) Nominated Officer (his deputy and the Prevention Unit);
(d) managers;
(e) employees involved in processing customers' instructions (financial operations);
(f) compliance and internal audit employees, if their area of competence includes the AML field;
(g) internal audit employees responsible for controlling all units, including the Nominated Officer and relevant employees.

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

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

(c) and (d) control activity of the NO and managers

Control activity is based on powers, duties and responsibilities of the NO and all managers of the financial institution and is performed as regular and ongoing activity of controlling the performance of work duties, consisting in the verification and approval of the quality, level or state of the performance of the work activities of subordinate employees in the AML/CFT field.

(e) control performed by employees

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

(f) control performed by employees performing compliance (internal control function)

The employees responsible for performing compliance (internal control function) control compliance with the Programme and internal regulations and verify AML/CFT procedures adopted, as well as the performance of duties by employees at various workplaces who execute, receive, process instructions for customers' financial operations, as well as the performance of duties by managers and the NO (his deputy and Prevention Unit).

(g) control performed by internal audit

The performance of internal audit control in the AML area should focus in particular on control of processes at all levels as well as control of the following:
1. the performance of the relevant degrees (levels) of customer due diligence;
2. procedures for ensuring that customers' information received is up-to-date (verification);
3. assessment of specific financial operations, monitoring of customers, their financial operations and business relationships;
4. risk evaluation and management;
5. internal notification of UTs and reporting of UTs to the FIU;
6. the implementation of staff training; and
7. records keeping.

The AML/CFT system and processes should be subject to internal audit, in accordance with the internal audit plan in such periodicity which will arise from evaluation of the degree of risk inherent in individual areas of financial institution's activity, at least once per calendar year. It should include evaluation of functionality, effectiveness and efficiency of all elements, tools, procedures, management and control mechanisms applied in this area.

(2) Members of the statutory body of the financial institution should be regularly informed of the results of controls and audits performed, e.g. once a year and immediately in the case of finding serious deficiencies.

PART III

Special provisions for activities of management companies

Article 14

(1) The provisions of Part II of this Methodological Guideline apply mutatis mutandis to the regulation of the management company's own protection within the activity consisting in collective investment. Own protection is to be based, in terms of its content and substance, on the basic principles and the concept of protection of the company with regard to specific characteristics of the company, such as its size, organisational arrangement, the management and scope of permitted and performed activities.

(2) The provisions of Part II of this Methodological Guideline apply to the activities performed by the management company under Article 27(3) of the AoCI (selected investment services and incidental services within the meaning of Article 6 of the AoSIS) in full.

Article 15
Duties of management company under depositary contract

(1) A management company (hereinafter referred to as the "MC") is required to provide for prevention of money laundering and terrorist financing, which also arises from the provisions regulating mutual relations with the depositary performing the activities under Article 70 of the AoCI.

(2) Subject to Article 71 of the AoCI, both the MC and the depositary are required, in concluding a depositary contract, regulate their mutual relations in a manner to ensure the exchange of information and obligations relating to confidentiality. Such contract should regulate and define the list of all information that will be the subject of exchange between the MC and the depositary in connection with the issuance, payment and cancellation of mutual fund shares. It is also necessary to determine the scope of obligations relating to confidentiality, secrecy, and protection of sensitive information, as well as to define the transfer of information about tasks and responsibilities of the parties in connection with their obligations related to prevention and detection of money laundering and terrorist financing.

PART IV

Special provisions for activities of pension funds management companies and supplementary pension management companies

Article 16

(1) The provisions of Part II of this Methodological Guideline apply mutatis mutandis to the regulation of the PFMC's and SPMC's own protection within the activity consisting in the establishment and management of pension funds and supplementary pension funds for the purpose of old-age and supplementary pension savings as defined in the AoOAPS and AoSPS. Own protection of a company is to be based, in terms of its content and substance, on the basic principles and the concept of protection of the company with regard to specific characteristics of the company, such as its size, organisational arrangement, the management and scope of permitted and performed activities.

(2) In the framework of the focus of their AML protection, a SPMC is mainly concentrated on payment of voluntary contributions to the old-age pension saving scheme under Article 20(b) of the AoOAPS from savers directly by the savers, and a SPMC is concentrated on payment of contributions directly by persons enrolled. In doing so, they fulfil their duties regulated by the Act in full, including customer due diligence, monitoring of the customer's behaviour, evaluation of the customer's risk rating, and subsequently the assessment of its activities beyond the defined customer's profile.

Article 17
Final provisions

This Methodological Guideline replaces in full the Methodological Guideline of the Financial Market Supervision Unit of Národná banka Slovenska No 5/2013 of 24 October 2013 regarding prevention against money laundering and terrorist financing within the activity of an investment firm, a branch of a foreign investment firm, a management company, a pension funds management company, and a supplementary pension management company.

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 AML Act and provides more detailed guidance on risk factors financial institutions should consider when performing customer due diligence.

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

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

Part 1
General guidelines on assessing and managing risk

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

Financial institutions should perform a business-wide assessment of ML/TF risks to understand where they are exposed to ML/TF risk and which areas of their business they should prioritise in the mitigation of these risks. In line with Annex 2 to the 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.

Firms should gather sufficient information to be satisfied that they have identified all relevant risk factors, including, where necessary, by applying additional customer due diligence measures, and assess those risk factors to obtain a holistic view of the risks associated with a particular business relationship or occasional transaction.

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 26a of the Act and 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 and legally non-binding lists (blacklists, etc.);

(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 assessments

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 their customer requires;
(c) the countries or geographical areas their customers operate in;
(d) the delivery channels used by the financial institutions to deliver products, services and transactions.

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

2.1.1. Customer risk factors

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

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

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

- Does the customer or beneficial owner have links to sectors that are commonly associated with higher corruption risk (such as construction, healthcare, the arms trade and defence, the extractive industries, public procurement, etc.)?

- Does the customer or beneficial owner have links to sectors that are associated with higher ML/TF risk (such as casinos, gambling venues or dealers in precious metals)?

- Does the customer or beneficial owner have links to sectors that involve significant amounts of cash?

- Does the customer have political connections (for example, are they a politically exposed person or is their beneficial owner a politically exposed person, do they have any links to a politically exposed person)?

- Does the customer or beneficial owner hold another prominent position or enjoy a high public profile that might enable them to abuse this position for private gain (for example, are they members of local or regional decision-making bodies with the ability to influence the awarding of public contracts, decision-making members of high-profile sporting bodies or individuals who are known to influence the government and other senior decision-makers)?

- Based on publicly available sources, is there evidence that the customer has been subject to sanctions for failure to comply with AML/CFT obligations?

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

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

- Are there adverse media reports or other relevant sources of information about the customer (for example, are there any allegations of criminality or terrorism against the customer or the customer's beneficial owner)?

- Has the customer, beneficial owner or anyone known to be closely associated with them had their assets frozen or the disposal with their assets limited in another way due to administrative or criminal proceedings or allegations of terrorism or terrorist financing?

- Does the financial institution know if the customer or beneficial owner has been the subject of an unusual transactions report in the past?

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

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

- Is the customer's ownership and control structure transparent and does it make sense? If not, is there an obvious logical or economic rationale to this?

- Is the customer established in or do the funds proceed from a country associated with higher ML risk (jurisdictions that do not comply effectively with international tax transparency standards)?

- Is there a sound reason for changes in the customer's ownership and control structure (such as sale or transfer of the company or a part thereof to other beneficial owners, etc.)?

- Does the customer request transactions that are complex, unusually large or have an unusual or unexpected pattern without an apparent economic or lawful purpose or a sound commercial rationale (for example, is the customer trying to evade specific thresholds set out for occasional transactions)?

- Is the customer reluctant to share obligatory customer due diligence information about themselves or their beneficial owner?

- Does the customer transfer funds in excess of the agreed transaction and ask for surplus amounts to be reimbursed?

- Does the customer use multiple accounts without previous notification, especially when these accounts are held in multiple or high-risk jurisdictions?

- Does the customer ask to redeem a long-term investment within a short period after the initial investment without a clear rationale, in particular where this results in financial loss?

- Does the customer request unnecessary or unreasonable levels of secrecy? Is the customer reluctant to share obligatory customer due diligence information, or does the customer appear to want to disguise the true nature of their business?

- Is the customer able to easily and logically explain to the financial institution the source of their wealth or the source of funds (for example through their occupation, business activity, inheritance, donation or investments)? Is the explanation plausible?

- 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 transparency:
- the products, services and transactions allow the customer or beneficial owner to remain anonymous, or facilitate hiding their identity (such as products and services that involve 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 complexity:
- a third party that is not part of the business relationship is able to give instructions for the execution of the transaction;

- the transaction is complex and involves multiple parties or multiple jurisdictions;
- there are risks associated with financial institution's new products, 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 at the financial institution);

(c) risks related to value or size:
- the products and services are cash intensive;
- the products and services encourage high-value transactions.

2.1.3. 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.

Where the funds used in business relationships have been generated abroad, financial institutions should have knowledge about the level of predicate offences to money laundering and the effectiveness of a country's legal system.

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

(a) 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 obligatory customer due diligence measures.
(b) 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 Financial Action Task Force (hereinafter 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 bodies similar to the FATF (e.g. MoneyVal) does not, of itself, mean that the country's AML/CFT regime is adequate and effective.
(c) 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.
(d) 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.
(e) 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 obtains the products or services they require, financial institutions should consider the following risk factors, among others:

- The customer is not physically present for identification purposes. If this is the case, 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. If this is the case, the financial institution should consider to what extent can it rely on this introduction as reassurance that the customer will not expose the financial institution to excessive ML/TF risk. The financial institution should verify whether the other institution of the same financial group applies obligatory customer due diligence measures to EU standards in line with Article 28 of Directive (EU) 2015/849.
- The customer has been introduced by a third party, for example a bank that is not part of the same group, and the third party is a financial institution or its main business activity is unrelated to financial service provision. 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 risk

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 relative 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: high, medium and low. More detailed categorisation is also possible, for example by splitting the “Medium risk” category into “Medium low risk” and “Medium high risk”.

Part 3
Management of ML/TF risks

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 Act, financial institutions may apply simplified obligatory 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 primarily include:

3.1.1. adjusting the timing of customer due diligence, for example where the product 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) this does not result in an exemption from obligatory customer due diligence, that is, financial institutions must ensure that the customer's or beneficial owner's identity will ultimately be verified;

(b) the threshold or time limit is set at a reasonably low level (although, with regard to terrorist financing, financial institutions should note that a low threshold alone may not be enough to reduce risk);

(c) they have systems in place to detect when the threshold or time limit has been reached;

(d) they do not defer obligatory customer due diligence or delay obtaining relevant information about the customer.

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

1) verifying identity on the basis of information obtained from one reliable, credible and independent document only; or

2) assuming the nature and purpose of the business relationship.

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

1) accepting information obtained from the customer rather than an independent source when verifying the beneficial owner's identity; or

2) where the risk associated with all aspects of the relationship is low, relying on the source of funds to meet some of the obligatory customer due diligence requirements (for example where the funds are state benefit payments).

3.1.4. adjusting the frequency of customer due diligence updates and reviews of the business relationship (for example carrying these out only when trigger events occur such as the customer looking to take out a new product or service or when a certain transaction threshold is reached).

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

Financial institutions should ensure that the information they obtain when applying simplified obligatory customer due diligence measures are sufficient to justify the low risk.

It must also be sufficient to give the financial institution enough information about the nature of the business relationship to identify any unusual or suspicious transactions. Simplified customer due diligence does not exempt the financial institution from its obligation to conduct ongoing monitoring of business relationships in order to detect UTs.

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 Act, financial institutions are obliged to perform enhanced customer due diligence where risk assessment under Article 10(4) of the 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:

1) where the customer is a politically exposed person;

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

3.2.1. Enhanced due diligence with respect to politically exposed persons

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

(a) Take adequate measures to establish the source of wealth and the source of funds to be used in the business relationship in order to allow the financial institution to satisfy itself 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 high 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 where the risk associated with the relationship involving a politically exposed person is particularly high.

(b) Obtain approval of the statutory body or Nominated Officer under Article 20(2)(h) of the 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 company'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 high-risk third countries and other high-risk situations

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 obligatory customer due diligence measures are appropriate for each high-risk situation.
Financial institutions are not required to apply all the enhanced obligatory 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.

3.2.3. 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 products or services; 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 obligatory customer due diligence measures should be sufficient to help the financial institution determine whether these transactions give rise to suspicion and must at least include:

(a) taking reasonable and adequate measures to understand the background and purpose of these transactions, for example by establishing the source and destination of the funds or finding out more about the customer's business to ascertain 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. Financial institutions can decide to monitor individual transactions where this is commensurate to the risk they have 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:
- 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;
- 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;
- obtaining the approval of the statutory body or a senior manager or the Nominated Officer to establish or continue the business relationship to ensure that senior management are aware of the risk their financial institution may be exposed to.

Other considerations with respect to enhanced due diligence

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

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 assess information obtained as part of their ongoing monitoring of a business relationship and consider whether this affects the risk assessment.

Financial institutions should also ensure that they have systems and controls in place to identify emerging ML/TF risks and that they can assess these risks and, where appropriate, incorporate them into their risk assessments in a timely manner.

3.3.1. Systems and controls to identify risks financial institutions should put in place include:

(a) processes to ensure that internal 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.);

3.3.2. Systems and controls financial institutions should put in place to ensure that their risk assessments remain up to date include:

(a) setting a date on which the next risk assessment update will take place to ensure new or emerging risks are included in risk assessments; where the financial institution is aware that a new risk has emerged, or an existing one has increased, this should be reflected in risk assessments as soon as possible;

(b) carefully recording issues that could have a bearing on risk assessments, such as internal suspicious transaction reports, compliance failures and intelligence from front office staff.

Any update to a risk assessment and adjustment of accompanying obligatory customer due diligence measures should be proportionate to the identified ML/TF risk.

3.3.3. Financial institutions should take steps to ensure that their risk management systems and controls, in particular those relating to the application of the right level of obligatory customer due diligence measures, are effective and proportionate.

3.3.4. 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 risk management measures are adequate.

ANNEX 2

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

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

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

1. Information on customers and circumstances of concluding the business relationship, or circumstances of the product or service provided, or transaction conducted, from the financial institution's front office staff;
2. Internal reports of UTs and records on them;
3. Information acquired in the course of the ongoing monitoring of the business relationship;
4. Information acquired in the course of the retrospective assessment of the customer's products, services and transactions;
5. Compilation reports and outputs from the financial institution's internal information system, which should be used by the financial institution to evaluate and identify signs indicating possible UTs and which must be harmonised with the Programme;
6. Information received from other obliged entities;
7. Information from commercial databases;
8. Information from open sources;
9. Information arising from requests and instructions of authorised entities, in particular the police force, prosecutor, courts, executors, etc.;
10. Information from the FIU, in particular feedback on the effectiveness of UT reports received and the manner of their handling, and warnings and information on indicators and new forms of UTs published by or targeted by the FIU;
11. 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 person;
3. The product, service, transaction and requests of the customer;
4. Other available and known relationships, circumstances and information acquired not only through the activity of the financial institution and its staff, but also through the activity of, e.g., competent authorities;
5. Decisions on a potential delay of UTs.

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

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

- Social status;

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

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

- The line of business in relation to the assessed product, service or transaction, as well as in terms of creating the customer's risk profile;
- Determining whether the legal person is an obliged entity;
- The form and statute of the legal person;
- The date and place of registration in relation to the increased level of risk (name-plate 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;
- Course of business to date;
- Frequent changes of the company's registered address and name;
- Available information from open sources;
- Unpaid obligations toward business partners and the state;
- 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;
- Degree of risk inherent in the product, service or transaction;

- Value and volume of the product, service or transaction;
- Subject of the product, service or transaction;
- Coverage of the product, service or transaction;
- Method and form of payment;
- Documents presented by the customer;
- Customer's requirements;
- Business partners,
- 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:

- Persons in the case of whom it may be presumed that they do not act on their own behalf and may be directed by another person, i.e. a "money mule", and persons in the case of whom the risk of money laundering and terrorist financing is higher than that in the general population. Such persons can be recognised in particular on the basis of the following external characteristics and features:
- Unkempt appearance, poor social situation;
- Influence of narcotics;
- Ignorance of the product, service, transaction or line of business;
- Unusual and abnormal behaviour;
- Homeless persons with registered permanent residence only at a local authority office; the street name is missing in documents, or this fact is known to the financial institution's staff;
- Persons who feature as the owner of several companies that have progressively been transferred to these persons over some time;
- Persons who, while being the true owner or executive of a company, nonetheless do not have disposal rights to the accounts or never act alone;
- The presence of third persons who direct or monitor the actions of such person;
- Persons using lost, falsified or altered documents;
- Persons intentionally giving false data, particularly on employment, place of residence, activities, etc.; also persons not responding to the financial institution's requests,
- Persons sought by police;
- Persons suspected of committing crime;
- Persons known or suspected to be a member of a criminal group;
- Persons on wanted lists of armed and intelligence services;
- Persons on lists of persons subject to sanctions,
- Persons on lists of terrorists or sympathisers of terrorism as such;
- Persons expressing through their appearance, behaviour or statements sympathy for extremism;
- Foreigners with no apparent relationship to Slovakia;
- Foreigners from areas known to be high-risk in relation to the promotion of international terrorism;

- Persons deprived of legal capacity;
- Children, youths, close to the age of a youth, and also elderly people;
- Persons with an increased risk of corruption – public administration representatives, representatives of political parties;
- Politically exposed persons, foreign public officers;
- 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;
- A "ready-made" company;
- In the case of other obliged entity – the indication of not devoting attention to the transactions of its customers;
- 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.;
- An empty shell bank;
- 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.

In relation to a product, service, transaction or request for their execution:
1. A product or service used, or transaction conducted 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 purpose 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. 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.);
8. A request by a customer for portfolio management services, where the source of funds is unknown or not consistent with the customer's apparent, in particular financial, situation;
9. Products, services or transactions involving limited liability companies in which there has been a change in the position of executive, a change of company name, a change of registration court, etc.;
10. Payment from abroad, particularly a country outside the EU, and its immediate transfer to a different account;
11. 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.

Forms of UT may involve in particular:

1. A product, service or transaction in which the customer refuses to provide information on imminent operations, or seeks to provide as little information as possible, or provides only information that the obliged entity can check with great difficulty or at high cost;
2. 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;
3. 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;
4. Frequent exchange of funds for other currencies (attempt to conceal the origin of the money through conversion to a different currency);
5. Repeated back-transfers of funds to and from foreign banks domiciled in high-risk areas or companies domiciled in high-risk areas;
6. Purchase and sale of securities outside the customer's normal practice without proper justification;
7. High or unusual settlement of securities in cash;
8. Purchase and sale of securities without discernible purpose or under circumstances that seem unusual;
9. Any transaction with an intermediary 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;
10. Products, services or transactions involving newly-incorporated companies registered in tax havens;
11. Involvement of a firm or financial institution from a high-risk country in a transaction.