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

The Financial Market Supervision Unit of Národná banka Slovenska, on the basis of Article 1(3)(a)(3) of Act No 747/2004 Coll. on financial market supervision, as amended, in collaboration with the Ministry of the Interior of the Slovak Republic, Ministry of Finance of the Slovak Republic and the Slovak Banking Association, has issued this methodological guideline:

P A R T I

Article 1
Purpose

(1) The purpose of this methodological guideline is to provide financial institutions explanatory material for fulfilling their duties arising under legal regulations focused on the prevention of money laundering and terrorist financing in the financial system, which are based not only on binding Slovak legislation, but also international standards and, not least, on knowledge, experience and practice gained in the performance of supervision and control by the NBS and FIU.

Financial institutions have been required since 1 September 2008 to comply with duties and exercise rights laid down by the Act, whilst proceeding also in accordance with other legal regulations, in particular Act No 483/2001 Coll. on banks and on the amendment of certain laws, as amended and Act No 492/2009 Coll. on payment services and on the amendment of certain laws, as amended.

In preparing this methodological guideline the authors have worked from the fact that the rules laid down by the legal regulations represent minimum requirements; the authors, through this methodological guideline, neither can nor seek to give instruction for solving all cases that arise in practice. The rules do, though, give financial institutions the freedom to use other sources of information and to set their own rules, if necessary more stringent than those required by Slovak legislation. In accordance with the objective pursued by the above-mentioned acts and by this methodological guideline, financial institutions may also use more sophisticated methods, particularly those already used and proven in their own practice or that of their parent companies from other member countries of the European Economic Area (hereinafter referred to as the "EEA"). In so doing they can better contribute to the implementation of the global AML/CFT policy in the framework of the financial group of which they are part.

(2) Financial institutions are, in the course of their business, exposed to the risk that customers will misuse the financial institution's services in the process of money laundering or terrorist financing. 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 a financial institution for money laundering or terrorist financing consist primarily in the integrity and honesty of the management and its commitment to actively enforce the financial institution's policy for the prevention and detection of money laundering and terrorist financing and to promote strict compliance with legal regulations relevant to these areas.

Article 2
Definitions

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

Act	Act No 297/2008 Coll. on the prevention of money laundering and terrorist financing and on the amendment of certain laws, as amended
AML or AML area	area regulated by the Act and International Sanctions Act
AML/CFT	Anti-Money Laundering/Combating the Financing of Terrorism
bank	legal person domiciled in the Slovak Republic as a joint-stock company pursuing activity in the Slovak Republic under Article 2 of the Banking Act
Banking Act	Act No 483/2001 Coll. on banks and on the amendment of certain laws, as amended
employee or staff	an employee (or collectively employees) of a financial institution performing tasks under the Act
financial institution	a bank or foreign branch
FIU	Financial Intelligence Unit, the Intelligence Unit of the Financial Police of the Slovak Police Force
foreign branch	a branch of a foreign financial institution or foreign credit institution pursuing activity in the Slovak Republic under Article 8 or 11 of the Banking Act
International Sanctions Act	Act No 126/2011 Coll. on the implementation of international sanctions, as amended
money laundering	the legalisation of proceeds from crime
Payment Services Act	Act No 492/2009 Coll. on payment services and on the amendment of certain laws, as amended
UT	unusual transaction

P A R T I I

Article 3
The policy of protecting a financial institution against money laundering and terrorist financing

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

(2) In setting and applying the financial institution's AML/CFT policy a suitable tool and valuable source of information are Slovak and international standards, opinions and guidelines of Slovak and foreign regulators, analyses by major Slovak and foreign institutions or consultancy firms, and not least also the experience and the approach of other companies within the group of which the financial institution is part. In creating the AML/CFT policy, the financial institution shall take into account its business objectives, existing clientele, range of banking activities and products (types of transaction) and the associated potential threat of their misuse for the purposes of money laundering and terrorist financing.

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

(4) Important components of the financial institution's AML/CFT policy are:
a) a programme of internal activities pursuant to Article 20 of the Act (hereinafter simply the "Programme");
b) an organisational structure ensuring effective and independent performance of AML activities;
c) 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.

(5) A bank's articles of association shall define the bank's organisational structure and bank's system of management, responsibilities of persons and units in the framework of managing risks to which the bank is exposed in its business. In determining the organisational structure pursuant to subparagraph 4(b) the bank shall designate a member of the statutory body as responsible for the area of AML (hereinafter referred to as the "Responsible Person"). The AML/CFT policy, in written form, shall be adopted by the statutory body, which is also responsible for implementing it.

(6) In determining the organisational structure pursuant to subparagraph 2, a foreign branch shall designate a managerial employee as responsible for the AML area, or shall designate that the head of the foreign branch is responsible for the AML area (hereinafter simply the "branch's Responsible Person"). The AML/CFT policy, in written form, shall be adopted by the branch's Responsible Person. The branch's Responsible Person is responsible for implementing the foreign branch's AML/CFT policy.

(7) The AML/CFT policy shall be published by the financial institution on its website.

Article 4
Employees responsible for implementing AML/CFT tasks

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

(2) A branch's Responsible Person is responsible for the prevention of money laundering and terrorist financing at the foreign branch and for implementing the AML/CFT policy.

(3) 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, the reporting of unusual transactions and for ongoing contact with the Financial Intelligence Unit lies with the Nominated Officer.

In banking terminology, or in the terminology of international institutions promoting the principles of the prevention of money laundering and terrorist financing, the term “anti-money laundering and counter terrorist financing compliance officer” is used, referring to the employee of the financial institution in charge of AML/CFT tasks. In view of the fact that the Slovak language has no adequate expression for this post, or function, the term “Nominated Officer”, or its abbreviation “NO”, is used in this methodological guideline in accordance with Article 20(2)(h).

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

(5) A financial institution shall ensure full substitutability for the post of the NO, by nominating a deputy NO.

(6) In filling the posts of the NO and deputy NO the financial institution shall require candidates to demonstrate civic integrity, appropriate education and corresponding professional experience.

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

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

Where a financial institution has several places in the Slovak Republic at which it performs an activity (branches, sub-branches, external posts, etc.) it may nominate an employee at these places, who need not be a member of the unit responsible for performing activities necessary for ensuring tasks of the preventive system (hereinafter simply the “Prevention Unit”), and entrust that employee with the performance of selected activities pertaining to the NO or Prevention Unit (hereinafter simply the “Authorised Employee”). The Authorised Employee is in continuous working contact with the NO. If a financial institution also establishes a Prevention Unit, the NO shall be the manager of that unit.

(9) The job description of the NO, or Prevention Unit, shall include in particular:

a) ongoing preparation and updating of the Programme and any other necessary regulations and procedures for the AML field;

b) the fulfilment of management and control tasks in the field that he performs and for which he is responsible in the framework of the Prevention Unit, if established in this field;

c) communication, cooperation and maintaining ongoing contacts with the Financial Intelligence Unit, including the timely reporting of UTs;

d) organisation and setting of rules for the training of the financial institution’s relevant staff, including new staff;

e) analytical and advisory activity in relation to the assessment and reporting of UTs by the respective staff in connection with the execution of customers’ transactions and financial operations.

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

The NO of a bank shall submit a report on his activity or on the activity of the Prevention Unit, if established, to the bank’s statutory body at least once a year.

The NO of a foreign branch shall submit a report on his activity, or on the activity of the Prevention Unit, if established, to the Responsible Person of the branch and to the head of the foreign branch at least once a year.

The activity report shall contain in particular the following information:

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

(11) An important element of AML/CFT policy is to ensure that the NO, his deputy and the Prevention Unit have a sufficiently independent status in the structure of managerial staff and organisational units. An NO's classification in a financial institution's organisational structure shall contain the following elements guaranteeing an appropriately defined standing of the NO, his deputy and, as relevant, the Prevention Unit:
a) arrangement of powers and duties of the NO and his deputy in their job descriptions, with emphasis on the primary area of their operation, which is to ensure the prevention and detection of money laundering and terrorist financing (other activities may not impede them in promoting effective measures in this primary area);
b) separation from units responsible for executing customers' transactions and financial operations,
c) unrestricted 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 unusualness of customers' transactions reported by the respective staff in the framework of the internal reporting system;
e) autonomous and independent decision-making on the sending of UT reports to the FIU;
f) control function of the NO, his deputy and of the Prevention Unit in relation to units and staff responsible for executing customers' transactions and financial operations;
g) separation of the NO, his deputy and Prevention Unit from the internal control and internal audit unit in the organisational structure, whilst preserving follow-up inspection of their activity conducted from the side of the internal control and internal audit unit;
h) cooperation with the internal control and internal audit unit in the procedure under Article 41(2) of the Banking Act; as well as the powers to participate in the process of commenting on or evaluation of new types of transactions (products) under preparation at the financial institution in terms of the risk related to money laundering and terrorist financing, and to express a dissenting opinion to introduced new types of transaction 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 of the branch.

Article 5
Financial institution's programme of internal activities

(1) A bank's articles of association, pursuant to Article 23 of the Banking Act, arrange the organisational structure and its internal system of management. A bank is obliged to clearly divide and arrange in its articles of association the powers and responsibilities at the bank for AML/CFT. The articles of association shall also arrange the system of risk management and the separation of risk management from management of banking activities. The arrangement of risk management shall include also a system of risk management, in which AML/CFT forms a component of operational risk.

(2) A financial institution shall draw up the Programme as an internal regulation, approved by the statutory body of the bank or head of the foreign branch. The Programme shall be based on generally binding legal regulations, in particular the Act, the Banking Act, NBS Decree No 13/2010 on additional types of risk, on details of the risk management system of banks and foreign bank

branches and on defining a sudden and unexpected change in market interest rates, and on the methodological guidelines of the FIU published and regularly updated on the website of the FIU (http://www.minv.sk/?aplikacia).

The Programme shall also take into account the bank's articles of association and the financial institution's AML/CFT policy.

The Programme shall represent 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. It shall also contain specific authorisations, duties, responsibilities and tasks of the NO, the Prevention Unit and relevant staff of the financial institution in the performance of banking activities, types of transactions and financial operations of customers in terms of statutory requirements (in particular Article 20(2) of the Act) that require the prevention of money laundering and terrorist financing, as well as the control powers of these subjects and control powers of the internal control and internal audit unit (see Article 12). The Programme shall also define information flows, information systems, control processes and mechanisms in this field.

(3) In creating the Programme the financial institution shall take into account its own specific characteristics, in particular its size and market share, organisational arrangement, the type and range of permitted and performed banking activities, the types of transactions and their range and specifics, the type and number of customers and the specifics and range of these customers' operations. The Programme shall contain not only information on statutory provisions, staff responsibilities, but also all operational procedures and duties of staff at the financial institution in the performance of the relevant type of customers' transactions and financial operations, as well as the most common types of UTs at the given financial institution.

(4) The Programme shall set out in particular:

a) the specification of tasks, duties and responsibilities for the financial institution's comprehensive prevention of money laundering and terrorist financing, at the individual levels of management from the board of directors of the financial institution, or from the Responsible Person of the foreign branch down to the units of first contact with the customer, including the Prevention Unit;

b) the nomination of the NO pursuant to Article 20(2)(h) of the Act;

c) the specification of persons at the financial institution who assess whether an intended or ongoing transaction is unusual;

d) the specification of the time when the assessment is to be performed (where possible, always before execution of a transaction or in the process of its preparation);

e) the specification of the method of performing assessment pursuant to points (c) and (d), i.e. to state what needs to be performed in an assessment, what aids are to be used (e.g. an overview of the types of UTs, publicly available information on debtors and defaulters, internal lists of customers, etc.), how and where to record the assessment result;

f) arrangements for the prevention of money laundering and terrorist financing, the receipt of notifications on identified UTs from organisational units, the evaluation of these notifications and the reporting of UTs to the FIU and arrangements ensuring ongoing working contact with the FIU, or law-enforcement bodies;

g) the specification of basic tasks of the respective staff at all levels of management, the detection of STs and the reporting of internal notifications of UTs to the NO (possibly also a specimen form for internal notifications of a UT) and the manner of ensuring the protection of the respective staff in connection with the UT they identified and reported to the NO;

h) the duty to identify customers in executing transactions and individual financial operations and the duty to verify this identification;

i) the duty to record the identification made and the verification of customer's identification, as well as all financial operations executed for customers;

j) the obligation to retain 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 by the Act;
k) an overview of known types of UTs, broken down by activity and type of transaction executed,
l) the evaluation and management of risks associated with money laundering and terrorist financing, including customer assessment procedures based on a risk-oriented approach and risk analyses, taking account of the results of initial and ongoing customer identification and verification of their identification, broken down by type of transaction and type of operation and account;
m) the specification of the nature and extent of the implementation of customer due diligence on the basis of risk evaluation results pursuant to Article 10(4) of the Act;
n) detailed signs of unusualness by which a customer's UTs can be recognised;
o) the manner and scope of feedback at the financial institution on internal notifications of STs;
p) the procedure of the respective staff and NO in postponement a unusual transaction under Article 16 of the Act;
q) the content and timetable of staff training, training staff for performing AML/CFT tasks in the performance of particular banking activities, types of customer transactions and operations;
r) the duty to maintain confidentiality regarding an internal notification of a 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 as provided for by the Act;
s) measures and control mechanisms preventing the abuse of position or function by staff to knowingly engage in money laundering or terrorist financing in the exercise of their function,
t) the method and periods for retaining data and documentation (see details in Article 11);
u) an internal control system focused on AML/CFT, consisting of control mechanisms, process controls of managerial staff, including controls by the NO and internal audits;
v) 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) The AML/CFT issue requires that the Programme be drawn up as an integral regulation accessible to all the financial institution's staff via an internal computer network.

(6) It is necessary to update the Programme not only in the case of a change in the relevant generally binding legal regulations, but also in the case of changes concerning the own performance of activity and transaction types, as well as in the case of changes to the financial institution's organisational arrangement. An appropriate period for updating is once a year.

Article 6
Staff awareness and training

(1) Managers and staff must be aware that both a customer's knowing facilitation and a customer's unwitting involvement through negligence in money laundering or terrorist financing represents an operational risk. The financial institution can ultimately suffer financial losses if it executes operations with proceeds from any criminal activity, whilst its reputation may also suffer. Not only financial institutions as legal persons are subject to penalties for a violation or failure to fulfil duties in this field, but members of the statutory body, supervisory board, head of a foreign branch, the Responsible Person of a branch, managerial staff performing control and the respective staff in direct contact with the customer and who execute the customer's instructions for performing transactions and financial operations may also be held liable.

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

(2) A financial institution shall publish in an appropriate manner information for staff as regards who performs the function of the NO and who deputises for the NO.

(3) A financial institution shall determine in the Programme the optimal regime and method for:
a) informing its staff about the AML/CFT system, and related procedures, duties and powers;
b) making the Programme and any other relevant regulations available to the respective staff;
c) organising regular staff training and educational activities for staff; where regular training is performed via e-learning, it is recommended in the case of finding the need to raise staff awareness of the Programme, to appropriately supplement e-learning training by personal or other training so that the training system is effective.

(4) The financial institution, in informing and training staff, shall take account of its conditions, in particular its size and organisational arrangement (branches, or other smaller workplaces), banking activities and types of transactions and financial operations performed for customers, so that all necessary information reaches all staff for whom the information is intended.

It is important that the mechanism of providing information to staff from the side of the statutory body, the Responsible Person of the foreign branch, the NO and respective managerial staff of the financial institution, as well as the model for performing staff training is effective, flexible and fulfils the desired objective; therefore it is essential that it be updated with regard to changing conditions.

(5) The effectiveness of a financial institution's prevention of money laundering and terrorist financing depends in large part on the level of knowledge on the side of management and staff 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 banking activities and types of transaction 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 staff (staff of first contact with the customer) must have all necessary information on the banking activities and types of transaction they execute for customers and they must learn as soon as possible the criteria (signs of unusualness) for assessing, or detecting, UTs. These staff must be able to assess the conduct of the financial institution's customers, as well as the content of financial operations performed by customers in terms of their degree of risk, unusualness or suspiciousness. Staff training should significantly contribute to staff acquiring the prerequisites for mastering procedures for applying the Know Your Customer principle (hereinafter referred to as "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 customer due diligence.

The relevant staff 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 UTs.

(6) Before an employee enters employment at the financial institution in a post or function where they will, in direct contact with customers, ensure the execution of financial operations, the financial institution shall check a copy of the potential employee's entry in the Criminal Register to establish that he has not been convicted of any property, economic or other serious crime. The financial institution may require from the potential employee information also beyond the framework of an excerpt from the Criminal Register, in so doing though, it should take account of the fact that pursuant to Act No 300/2005 Coll., the Criminal Code, as amended, if the conviction of a person has been expunged, this person is to be viewed as having a clean criminal record. The financial institution should require from a potential employee also a sufficiently satisfactory reference, or assessment of his prior work integrity, issued by his previous employer.

(7) In the framework of training, the financial institution shall ensure that staff 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 a UT.

(8) The financial institution must have a project or plan of staff 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 shall observe the provisions of Article 20(3) of the Act (once per calendar year and always before an employee is assigned to work in which he performs tasks under the Act). The plan of training, or its basic principles, should form a part of the Programme and should determine the basic outline, periodicity and content of staff training, in particular the provisions of the respective acts, internal regulations and rules of the financial institution or group to which the financial institution belongs, as well as an analysis of the content and circumstances of the most frequently occurring types of internal notifications of UTs within the financial institution, or within the group.

(9) The financial institution is required under Article 20(3) of the Act to ensure staff training focused on familiarisation with the Programme at least once per calendar year and always before an employee is assigned to work in which he will perform tasks set by the Act and by the Programme. Each competent employee 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 the Programme.

Staff training shall include in particular:

a) familiarisation with the Programme;

b) 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 supervisory authority.

Specialised training that staff 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 execution of transactions and operations. Through participation in training events (seminars, educational stays) staff shall 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.

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 staff are able to continuously perform their duties and exercise their powers. Forms of training (classic lecture, electronic, or other) should be regularly alternated. It is appropriate that the relevant staff be tested on the knowledge acquired.

(10) A financial institution shall draw up records on staff training conducted, containing the date the respective staff 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 staff a written or electronic confirmation that they have been familiarised with the Programme and related regulations governing AML/CFT procedures.

Article 7
Information system at a financial institution

(1) A systematic approach to the financial institution's risk management and AML/CFT requires the creation of appropriate information flows for ensuring the smooth, timely and regular flow of information between individual levels of management at the financial institution, including its statutory body, the NO, the deputy NO and the Prevention Unit, the internal control and internal audit unit and the relevant staff. A systematic approach for ensuring information flows also requires support in the form of application software, i.e. a specialised information system, or systems. In broad terms this means a system of acquiring, processing, evaluating, transferring and also using information concerning this area. This shall include flows of AML/CFT information in the processes of the financial institution's individual activities and types of transaction performed. For effective prevention it is essential to ensure that it is regularly updated, with emphasis on the timely introduction of new types of transaction (which, prior to their inclusion in the existing range of banking products 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.

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

(2) The financial institution is required to ensure information flows for:

a) the transmission of information to staff on AML/CFT principles, procedures, duties and powers and the related performance of day-to-day tasks;
b) making the Programme and other relevant internal regulations available to employees;
c) transmission of necessary information between the Responsible Person and NO;
d) transmission of information between staff and the NO and vice versa, including the internal reporting of UTs;
e) record-keeping, i.e. the recording, processing and updating of data on customers and the recording and monitoring of customers' transactions;
f) 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 staff of these results,
g) 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 UTs in the financial institution's relevant information systems that contain data on customers and their operations.

(3) 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 by it, 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 24(4) of the Act) as an obliged entity.

(4) 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 in the prevention of money laundering and terrorist financing.

An EIS, recording and processing data on customers and their financial operations must take account of the requirements provided for in Article 9(e) of the Act:

a) in the case of a natural-person customer, the EIS must contain records of at least the first name, last name, date of birth or birth registration number and the customer's account numbers, and in the case of a sole proprietorship also the identification number, if assigned;

b) in the case of a legal-person customer, the EIS must contain records containing at least the customer's name (business name) and identification number.

The EIS must also contain information or records on the nature of the customer's business relationship. The nature of a business relationship is given by the type of transaction pursuant to Article 9(i) of the Act or solely by a transaction pursuant to Article 9(h) of the Act, whilst the nature of the business relationship is primarily predetermined by the actual product or service that the customer uses. The EIS and the manner of using it should make it possible to identify UTs 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 unusual transactions of different customers.

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(d)) and Article 24(1) of the Act), which the respective staff received in performing their work tasks.

The EIS may also serve the financial institution for the needs of monitoring the necessary data for the purpose of keeping a register of unusual customers pursuant to Article 92(7)(a) of the Banking Act and for exchanging information with other financial institutions under Article 92(7)(b) of the Banking Act. Other situations in which the financial institution may use the EIS in providing information arise from Article 18(8) of the Act.

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 24(4) of the Act).

The EIS should also be capable of providing in a timely manner and sufficient scope data to the FIU, the Národná banka Slovenska – Financial Market Supervision Unit as the supervisory authority and law enforcement authorities in cases specified by the Act.

Last, but not least, the EIS should satisfy requirements for the purposes of control for the bank's own needs and for the needs of the FIU (Article 30 of the Act) and for statistical purposes.

Article 8
Client identification and customer acceptance, customer risk profile; basic, simplified, enhanced customer due diligence, performance 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, Article 89 and Article 93a of the Banking Act and Articles 31, 80, 88, and 88a of the Payment Services Act.

(2) A financial institution shall perform 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.

In the case of one-off transactions outside of a business relationship, the financial institution shall identify and verify identification always if the transaction value is at least €2000.

It shall observe the duty to ascertain whether the customer is acting on their own behalf. For the purposes of this methodological guideline the "execution of a transaction on the customer's own account" or with their "own funds" should be understood as the customer acting on their own behalf. According to Article 10(10) of the Act it is necessary to ascertain this fact always in the situations referred to in Article 10(2) and in accordance with Article 89(3) of the Banking Act even where this concerns a transaction at least in the amount of €15 000 (i.e. not only an "occasional" transaction as implied by the Act).

(3) The process of determining and, to an appropriate extent also verifying, the beneficial owner is governed primarily by the provisions of Articles 9 and 10 of the Act, whilst also the Banking Act partially addresses this important element of basic and enhanced customer due diligence in Article 93a. This means that it is always necessary to determine the beneficial owner in the case of legal persons, whilst the legal form of a company (e.g. joint-stock company with bearer shares or an asset pool) may not obstruct the detection of the beneficial owner. Verification of information acquired on the beneficial owner in accordance with the Act should be performed to an appropriate extent, e.g. by requesting a written declaration on the beneficial owner 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 beneficial owner on the basis of information from available sources, without the need to contact the customer or verify this information with the customer.

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

To illustrate possible situations in determining the customer's beneficial owner in the case of legal persons there is 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).

(4) The importance of the provisions of Article 10(1)(a) to (c) and Article 10(10) 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 a new customer, terminate an existing business relationship with a customer, or refuse to perform a specific transaction in the case where it is not possible to perform basic customer due diligence.

A comparable duty arises also under Article 89(1) of the Banking Act. Under Article 17(1) a financial institution is required to immediately report such cases to the FIU.

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

(5) 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.

In applying basic customer due diligence, a financial institution may not enter into 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. Managers and staff of a financial institution must know its customers and their usual commercial, business or other activity. Based on the information acquired, staff 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 shall 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 shall appropriately verify these facts.

The financial institution shall continuously update the customer's risk profile according to the risk group to which the customer is assigned; for this purpose it shall require from the customer the updating of data that the customer originally provided it, 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 performed by the financial institution 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 notify the financial institution of relevant changes.

(6) By means of categorising customers according to their risk profile the financial institution can then in practice apply Article 10(1)(d) of the Act, namely ongoing monitoring of the business relationship, which leads to recognition and also reporting of STs. (6) In connection with the risk categorisation of customers, the financial institution should consider also Article 10(1)(d) and Article 10(8) of the Act, which establish the duty to continuously update the customer risk profile on the basis of 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 the internal regulation arranging the Programme.

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 Financial Action Task Force (the intergovernmental body is the lead institution in setting international standards in the fight against money laundering and terrorist financing on a global scale; hereinafter referred to as 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 available on the website (http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/documents/fatfpublicstatement-19october2012.html); i.e. the "black list";

b) Improving Global AMLCFT Compliance: ongoing process available on the website (http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/documents/improvingglobalamlcftcomplianceongoingprocess-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 Public Statement 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 financial police intelligence (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 ("CPMLTF" – 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).

(7) 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.).

(8) Enforcement and compliance of all these procedures and rules (identification, verification, KYC) provides, besides the recognition of STs and minimisation of the risk of money laundering and terrorist financing, also protection against fraud. At the same time it enables the financial institution to select and offer from the range of transaction types those that are suitable for particular customers according to the content and scope of their activities. This helps the financial institution retain customers not connected with money laundering and fraud and concurrently eliminate the risk of financial loss and reputational risk.

(9) 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 shall exercise enhanced customer due diligence in situations that, with regard to their nature, may pose a high risk of money laundering or terrorist financing. The financial institution shall pay 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 corporations (Article 25(2)) and shell banks (Article 24(1)).

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 the consent of a managing employee, meaning an employee one or more management levels higher must be required for continuing the business relationship. Where a politically exposed person owns or works in the managing structure of a customer – legal person, or is a beneficial owner, in such a

case this constitutes a situation requiring the application of enhanced customer due diligence toward the customer – legal person.

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

A financial institution shall apply enhanced customer due diligence also if it is preparing to establish:

a) a new business relationship or account without the customer being physically present, and
b) new correspondent relationships with foreign banks or credit institutions outside the EEA.

A correspondent relationship is, pursuant to the definitions of the new FATF standards, the provision of banking services by one bank (the "correspondent") to another bank (which in this relationship is the "respondent"), where one of the usual mutually provided services is the opening of nostro and loro accounts in different currencies.

In assessing the risk of foreign banks or foreign credit institutions from a non-member state in the situation where the financial institution seeks to commence a correspondent relationship, it is recommended, in accordance with the European standard, to require and analyse, in addition to the information defined in Article 12(1)(b) of Act, also the documenting of duties and powers in the AML/CFT field, where in so doing it is important to add this information within an appropriate period also in the case of existing correspondent relationships.

(10) The Act in Article 13 allows the use of basic 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 the ongoing monitoring of a business relationship under Article 10(1)(d) of Act. This means that, as regards compliance with the conditions referred to in this provision of the Act, 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.

Bureaux de change 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 data 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 introduction.

(11) In Article 11 the Act defines the scope and conditions for exercising simplified customer due diligence; it must be emphasised here that this concerns the possibility to apply a less demanding procedure in customer identification.

The financial institution may use this option after careful consideration with the use of a risk-based procedure in the case of such situations and customers where it is possible to obtain and verify basic information from publicly available and reliable sources – as referred to in Article 11(1) of the Act.

Article 11(2) of the Act lays down the types of product in which simplified customer due diligence approaches may be used.

It is important that before deciding to use simplified customer due diligence the financial institution first obtain information about the customer or type of transaction (product) that justifies the application of simplified customer due diligence.

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)(d) of the Act), or from other duties defined by the Act, so that it is possible to comply with the provisions of Articles 14 and 17 of the Act, as well as others, including the duties to process and archive data according to the provisions of Articles 19 and 21 of the Act.

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 CPMLTF website, and on the FIU website. The fact that a country is included in the list, however, does not preclude that a particular 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 (8) of the Act.

Article 9
Detection, reporting and postponement of UTs

(1) For identifying UTs it is crucial that a financial institution apply the provisions of Articles 2 to 4, 10 to 12, 14 and 20 of the Act.

Under Article 14(1) of the Act of 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 be archived for 5 years on the basis of Article 30(3) of the Act in conjunction with Article 33(4) of the Act.

(2) Under Article 4 of the Act a UT is a legal act or other act that indicates that its execution may lead to money laundering or terrorist financing.

Article 4(2) of the Act gives a demonstrative presentation of UTs. In each UT listed in this provision there are, however, several indicators of unusualness (e.g. an unusually high volume of funds with regard to the type of transaction, an unusually high volume of funds without clear economic or legal purpose, etc.) that the financial institution is required to assess 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 or is not unusual. 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 a UT. The decisive element for assessing a customer's transactions is the application of the KYC principle and the proper recognition of indicators of unusualness, as well as other signs or criteria that the financial institution is required to determine for itself, depending on the subject and scope of its activity and the type and extent of transactions and financial operations performed for customers, in the framework of drawing up an overview of the types of ST (Article 20(2)(a) of the Act).

(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 the provisions of Articles 10 to 12 of the Act. The crucial provisions are those of Article 10(1), (4) and (5) and Article 11(3) of the Act.

The procedure under the provisions of Article 10(1) and Article 11(3) of the Act enables a financial institution to satisfy itself 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, and then determining the degree of customer due diligence pursuant to Article 10(4) of the Act and for accepting a customer. A financial institution then, depending on the result, shall apply procedures in the framework of basic customer due diligence under Article 10 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) Irrespective of whether a financial institution proceeds under Article 10, 11 or 12 of the Act, it is required always to also proceed in accordance with Article 14 of the Act. 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 in accordance with Article 14(3) of the Act (i.e. internal reporting of a UT); it is also necessary to archive these records in accordance with the period referred to in Article 19 of the Act.

(5) A financial institution shall perform skilled assessment of intended and ongoing transactions under Article 14 of the Act at various time intervals and at various levels. The assessment process takes place:
a) on the frontline, where the financial institution's staff are in contact with an existing or potential customer;
b) in the framework of ongoing monitoring of an existing business relationship;
c) in the framework of subsequent (retrospective) assessment of a customer's transactions.

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

The assessment of a customer's transactions is performed by staff of the financial institution who, in fulfilling their duties, are in contact with the customer, particularly those staff who receive or process a customer's instructions for execution of the customer's transactions or financial operations. This means in particular cashiers, staff arranging the execution of money transfers, or payments and other staff involved in the provision of services to customers and processing of data, as well as their direct superiors. 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 performance, or at an attempt to execute a transaction so that a UT can be postponed and promptly reported. The assessment of transactions is dependent on the staff's expertise and knowledge that they have acquired in the framework of mandatory training (Article 20(3) of the Act).

Each of the relevant staff 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 is governed in this stage primarily by Article 10(1) as well as by 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 commercial 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.

Another crucial element for assessing a customer's transactions is the appropriate application of the KYC principle and its procedures and skilled identification of signs of unusualness. This procedure enables the employee to assess a customer's intended or ongoing transactions by comparing them against an overview of types of UTs (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 customer and his otherwise usual transactions.

If an employee judges an intended or ongoing transaction to be unusual, he shall 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 simply "notification of a UT").

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

Depending on whether this concerns:

1. contracting of a business relationship (Article 10(2)(a) of the Act), or
2. an occasional transaction (Article 10(2)(b) and (c) of the Act),

the competent staff of the financial institution shall 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 arisen 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). This, therefore, is not the first contact with the customer and the financial institution may take account of the customer's existing risk profile and 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(8) of the Act and the customer's duty under Article 10(5) of the Act form the basis for ongoing monitoring 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. Ongoing monitoring of the business relationship requires the use of an appropriate EIS that enables the financial institution, in accordance with risk-based prevention, to create financial or other criteria or limits as indicators of unusualness in customers' transactions so as to allow their differentiation into certain levels of the monitoring process, corresponding to the degree of risk inherent in the operations performed by customers. The 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 shall 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 UTs referred to in the Programme or in Article 4(2) of the Act. Such transactions of a customer shall form the subject of assessment (Article 14(2) of the Act) and it is necessary to make a written record of them (Article 14(3) of the Act); these records must be archived in accordance with the period referred to in Article 19 of the Act. The NO may, on the basis of results from the assessment of the various circumstances of a transaction, and with regard to the overview of types of UTs (Article 20(2)(a) and Article 4(2) of the Act reach the conclusion that in the given case it does not constitute a UT. If this is not possible, solely on the basis of 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 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 proceed according to Article 17 of the Act, i.e. to report the UT to the FIU.

The assessment of transactions in the framework of ongoing monitoring of the business relationship is performed, depending on the transaction, by staff 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 subsequent monitoring of customers' transactions is, for example ex-post random selection of executed transactions in the framework of an inspection from the side of a manager superior to the employee who executed the customer's instructions and operations, as well as in the framework of an inspection performed by the NO and internal control unit (see part I).

(6) The recommended procedure in the processing and handling of internal notifications of UTs and UT reports is as follows:
a) All internal notifications of UTs sent by competent staff 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 Nominated Officer may not be subject to the prior consent of any person.
c) The NO shall register and archive notifications on internal notifications of UTs, including the position, first name, last name, branch or unit of the financial institution and all data on the given customer and transaction in accordance with Article 2 of the Act.
d) The NO, as well as staff of the financial institution, including its managers (and members of the statutory body) involved in assessing transactions under Article 14 of the Act are required to maintain confidentiality on reported UTs and on measures taken by the FIU (Article 18 of the Act), including the fulfilment of duties under the provisions of Article 17(5) and Article 21 of the Act; the financial institution may not, however, cite toward the Národná banka Slovenska and the Slovak Ministry of Finance 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 shall not apply to the provision of information between credit or financial institutions under the conditions set out in Article 18(8)(a) and (e) of the Act.
e) The financial institution is required to draw up a procedure covering the period from the moment of detecting a UT through to prompt reporting of the UT, including the procedure and responsibility of staff who assess the transaction.
f) The NO, after receiving an internal notification of a UT, may confirm receipt of the notification on the UT to the member of staff who sent the notification. The confirmation should contain an instruction on the duty to maintain confidentiality under Article 18 of the Act. Where the financial institution has an electronic system of gathering internal reports that enables the competent member of staff to monitor the status or receipt of a submitted internal report of a UT by the Nominated Officer, or by the Prevention Unit, no individual confirmation of receipt of such a notification is needed.
g) The internal notification of a UT, or the conduct of a customer, the transaction or financial operation that the notification concerns shall be 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 UTs (Article 20(2)(a) of the Act) and Article 4(2) of the Act, decide whether it does or does not constitute a UT. This internal notification shall contain information on the economic or lawful purpose of the transactions and, in the case that it is a usual transaction, also sufficient reasoning or statement of information and reasons regarding its usual nature. Otherwise the process of such assessment cannot be considered trustworthy and objective. If it is not possible to reach a decision solely on the basis of 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 a 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 a UT, it is sufficient that the transaction or financial operation indicates that its execution may constitute money laundering or terrorist financing, and the NO is required to proceed according to Article 17 of the Act, i.e. to report the UT to the FIU.

According to Article 17(1) of the Act a UT or attempt at executing a UT must be reported to the FIU promptly, i.e. at the earliest opportunity. It is always necessary to take into consideration the particular circumstances of the situation in which the finding of the UT is made, whilst a financial institution is required to report a UT as soon as possible. The decision of the NO to report a UT may not be subject to the consent or approval of any other person. A report of a UT shall contain data specified by the provisions of Article 17(3) and may not contain data referred to in Article 17(4) of the Act. The reference number of each report of a UT should take the form: serial number / year / character code of the financial institution, e.g.: 1/2009/SUBA.

A UT may be reported in writing, electronically or by telephone (in this case it is necessary to report the UT also in person, in writing or by e-mail). The specimen form for reporting a UT, issued by the FIU, is given on the website http://www.minv.sk/?vzory.

A UT 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 UT the financial institution shall state the UT to which the additionally acquired information and documentation relate.

In connection with the reporting of UTs 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 the transmitted data and 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,
i) The financial institution may, under Article 92(7)(a) of the Banking Act keep a register of customers whose conduct has been assessed as constituting a UT and against whom international sanctions apply, and under Article 92(7)(b) of the Banking Act may provide, without the customer's consent, information from this register (under the condition of protection of the provided information) to other financial institutions.
j) Article 18(8)(a) of the Act allows financial institutions, under defined conditions, to exchange information where this is reasonable and related to the threat of money laundering or terrorist financing, and where it helps obliged entities to more effectively assess a customer's transactions, as well as to alert other obliged entities to identified risks. An exchange of information may not contain the full scope of the reported UT as a whole, but only specific information relating to the risk of money laundering or terrorist financing. Information provided may, pursuant to the Act, be used exclusively for the purposes of preventing money laundering or terrorist financing.

(7) The recommended procedure in the postponement of a UT is as follows:
a) According to Article 16 of the Act, a financial institution shall postpone a UT, i.e. a particular transaction (Article 9(h)) of the Act that would otherwise be executed.
b) Unless there is from the side of the customer an act or expression of will to execute a transaction or operation, e.g. where the customer does not enter any payment order, does not make any withdrawal of funds from the account, etc., the financial institution has no transaction to postpone.
c) The financial institution is required under Article 16(1) of the Act to postpone a UT until the time of its reporting to the FIU, whilst account shall always be taken of the operating and technical possibilities, as well as the moment when the transaction was or should have been assessed as unusual; e.g. a customer's transaction assessed in the framework of ex-post or retrospective assessment of the customer's transactions can no longer be postponed.

d) The financial institution is required under Article 16(2) of the Act to postpone a UT in the following two cases:
1. the financial institution shall postpone a UT at its own discretion if execution of the UT poses the risk that there may be frustrated or substantially impeded the seizure of proceeds from crime or seizure of funds intended for financing terrorism; in such a case the financial institution is required to immediately inform the FIU of the postponement of the UT;
2. the financial institution shall postpone a UT if the FIU requests it to do so in writing; the reason for postponing a UT from the side of the FIU shall always be stated in the written request.
e) The financial institution shall not postpone a UT if it is unable to do so for operating or technical reasons (it shall immediately notify the FIU of this fact) or if postponing the UT could, according to a previous notice from the FIU, frustrate the processing of the UT.
f) The period of postponement of an operation pursuant to Article 16 of the Act shall be at most 48 hours; therefore, if during this period the FIU notifies the financial institution that it has forwarded the case to the law enforcement authority, the financial institution is required to extend the period of postponement, though at most by a further 24 hours.

The total duration of postponement of a UT is, therefore, at most 72 hours. In the case that during the period of postponement of an operation the financial institution receives no instruction to seize funds from the side of a judge or prosecutor pursuant to Article 95 or 96 of Act No 301/2005 Coll. the Code of Criminal Procedure, as amended (hereinafter referred to as the "Code of Criminal Procedure"), the financial institution shall execute the postponed operation following the expiry of the set period. Prior to the expiry of the postponement period, 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 UT, its further postponement is not necessary. Weekends and bank holidays shall not be counted in the period of postponement of a UT.

The period of postponement an operation pursuant to Article 16 of the Act shall be deemed to begin as of when the customer expresses the intention (will) to handle funds on an account. In the case that the financial institution presumes that the customer will express an intention to execute a UT (handle 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 postponement of the UT is not frustrated.

The period of postponement of an operation pursuant to Article 16 of the Act may not be deemed to begin as of when the financial institution evaluated the executed transactions as unusual, or learnt of the customer's executed operations. Likewise, the reason for postponing 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 10
Measures against 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.

(1) Definitions of terrorism and 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.

The aim of sanctions is to maintain or restore international peace and security according to the principles of the UN Charter and Common Foreign & Security Policy. This primarily concerns changing the policy of a government, state, individual or group that does not respect the fundamental principles of the rule of law, that breaches human rights, international law or threatens security.

(2) Procedure in fulfilling the reporting duty:

a) financial institutions shall, in the framework of CFT, apply toward customers procedures analogous to those applied in AML, including the reporting of UTs connected with terrorist financing to the FIU;

b) financial institutions are required to report UTs to the FIU promptly (Article 17(1) of the Act); the Act defines UTs 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 is a transaction in which there is a reasonable assumption that the subject of it is or should be a thing or service that may relate to a thing or service against which sanctions are imposed under the International Sanctions Act;

c) financial institutions are required, under Article 91(8) of the Banking Act to provide the Ministry of Finance of the Slovak Republic within the terms set by it (quarterly) a list of customers subject to international sanctions under the International Sanctions Act and relevant decrees. The list shall also contain the account numbers and account balances of these customers (hereinafter referred to as "persons subject to sanctions").

(3) Permission for funds transfer

Under Article 4(2) of the International Sanctions Act in conjunction with the respective EU Council Regulation on restrictive measures (e.g. EU Council Regulation No 961/2010 on restrictive measures against Iran) the Slovak Ministry of Finance is competent for the official procedure; e.g. to issue permits for a funds transfer following approval by other state bodies referred to in Article 14(5) and (6) of the International Sanctions Act. The requested authority is required to send an opinion within the term set by the Slovak Ministry of Finance, and this term may not be shorter than 10 days from delivery date of the request. A shorter period may be set only in exceptional cases and must be thoroughly justified.

The competent unit is the **Financial Market Section of the Ministry of Finance, Banking Department**, telephone contact: (02) 5958 2545, or (02) 5958 2541.

(4) Consolidated list of persons subject to sanctions

Lists of persons subject to sanctions (natural persons and legal persons) form a part of the annexes to individual regulations and decisions of the European Union (hereinafter referred to as the "EU"), which obligate all financial institutions of Member States to immediately freeze financial and economic resources of persons subject to sanctions from states listed in the annexes to the individual regulations and decisions of the EU.

The 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 http://eeas.europa.eu/cfsp/sanctions/index_en.htm. In this regard, the EU sanctions are listed on the website of the Ministry of Foreign Affairs of the Slovak Republic, (http://www.foreign.gov.sk/sk/zahranicna__politika/europske_zalezitosti-sankcie_eu, http://eeas.europa.eu/cfsp/sanctions/docs/measures_en.pdf).

(5) Adoption of sanctions (restrictive measures):
a) through the transposition of sanction resolutions of the Security Council of the United Nations (hereinafter referred to as the "UN Security Council");
b) in the case of autonomous sanctions adopted only by the EU, the sanctions are adopted through common positions of the EU and implemented at the EU level; in the case of autonomous sanctions, the EU may adopt also more stringent and broader sanctions than those of a sanction resolution;
c) sanctions concerning persons against whom they were declared pursuant to a regulation of the Government of the Slovak Republic.

Restrictive measures are adopted in several forms. This concerns, for example, diplomatic sanctions, suspension of cooperation with a third country, boycott of sporting or cultural events, trade sanctions, arms embargoes, financial sanctions, flight bans, restrictions on entry to the territory of a member state. UN sanction measures concerning an arms embargo or visa bans are implemented directly by the member state.

Sanction measures concerning economic relations with third countries, for example freezing of financial assets and economic resources, are implemented by an EU regulation (approved by the Council) 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 financial institutions in Slovakia are required to directly apply sanctions declared in EU regulations. They are also the subject of legal assessment by European courts.

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 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 the 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 everyone 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 toward third countries (Article 60 and 301 of the EU Treaty, i.e. it does not have a mandate to introduce financial sanctions at the Community level against the EU's own citizens). Against internal terrorists there is applied at the EU level only enhanced judicial and police cooperation on the basis of Article 4 of the EU Common Position 2001/931/CFSNP, and concurrently 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 regulation 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.

With regard to the above, the Slovak Republic has not been able to declare sanctions against internal terrorists of the EU, therefore it has been necessary to codify at the level of national legislation the freezing of terrorist assets of such persons. 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. Such an act, under Article 288 of the Consolidated Text of the EU Treaty is a Regulation having 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 Coll., No 484/2006 Coll., No 488/2007 Coll. and No 239/2008 Coll., 168/2009 Coll. and Decree No 442/2009 Coll. (hereinafter referred to as "Decree No 397/2005 Coll."). Decree No 397/2005 Coll. 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 Slovak Government Regulation No 397/2005 Coll. or in the relevant EU regulations governing restrictive measures.

Article 11
Archiving of data and documentation

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

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

(3) Financial institutions shall store (archive) data on the identification of customers and on the verification of identification, records on customers' transactions and financial operations and records on ascertaining beneficial owners, including photocopies of relevant documents.

(4) Under Article 19(1) and (2) of the Act, financial institutions are required to archive for the period of five years:
a) from the end of the contractual relationship with a customer, data and written documents acquired by way of the procedure under the provisions of Articles 10 to 12 of the Act;
b) from the execution of a transaction, all data and written documents on the customer.

(5) In view of the importance of the information acquired in fulfilling AML/CFT duties under Article 14(2)(a) of the Act, financial institutions are recommended to archive for the statutory period (5 years from the written record being made) also written records referred to in paragraph 3 of the mentioned Article.

(6) Financial institutions are required to archive this data and written documents also for longer than five years if the FIU requests it do so by way of a written request containing the period and scope of archiving data and written documents.

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

(7) The procedure followed by financial institutions in archiving data and documentation, and records relating to AML/CFT shall be governed by the financial institution's Programme, which should, in accordance with the Act, set out in detail:
a) the records that need to be archived (at least data on customer identification and records on customer transactions, including written records under Article 14(3) of the Act and data on identification of beneficial owners);
b) the form of records (paper, electronic);
c) the place, manner and period for which records are to be archived, taking account of
1. the end of the contractual relationship with the customer,
2. the execution of a transaction with the customer, and
3. any written request of the FIU and period specified under Article 19(3) of the Act.

a) records that need to be archived

1. records on customers' risk rating

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

2. 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 shall contain the customer's instructions related to the customer's payments.

The financial institution shall archive records on each financial operation made by the customer, including single financial operations performed for customers who do not have an account open at the financial institution. The archiving period in this case is the same as for archiving identification records and documentation.

3. records on internal notifications of UTs and UT reports

The financial institution shall archive 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 a 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.

4. Records on education and training

The financial institution shall archive 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, manner and period for which records must be archived

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

In view of the need to additionally provide data on customers and customers' financial 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 shall archive such information and documents also following the expiry of the statutory term for those customers and their financial operations in the case of which an investigation has been launched by 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.

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

(8) Records prepared and archived by the financial institution shall 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 UTs and external UT 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 12
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 shall comprise a specification of control responsibilities at all levels of the management and performance of banking activities, as well as the performance of control activity itself by:
a) the bank's supervisory board;
b) members of the bank's statutory body;
c) the Nominated Officer (his deputy and Prevention Unit);
d) managerial staff;
e) staff involved in the processing customers' instructions (financial operations);
f) the internal control and internal audit unit, which shall be responsible for controlling all units, including the NO, Prevention Unit and relevant staff.

a) and b) control performed by the bank's statutory body and supervisory board

Control shall be based on generally binding legal regulations and internal regulations of the financial institution and derive from the position in the hierarchy of the financial institution's management system. The statutory body of a bank and Responsible Person of a branch shall regularly, at least once a year, evaluate the effectiveness of the existing system – the AML/CFT policy, the Programme and specific measures, including the activity of the relevant units and staff.

c) and d) control activity of the NO and managerial staff

Control activity shall be based on powers, duties and responsibilities of the NO and all managerial staff of the financial institution and shall be 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 staff in the field of AML/CFT.

e) control performed by staff

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 staff working procedures as well as their work duties, tasks and responsibilities in first contact with customers, as arise from AML/CFT.

f) internal control and internal audit

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

The performance of control should be focused primarily on checking:
1. the performance of the relevant degrees of customer due diligence;
2. procedures for ensuring that customer information received is up to date (verification);
3. assessment of specific financial 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. performance of staff training; and
7. record keeping.

The AML/CFT system and processes should be subject to regular internal audit, which should evaluate the 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 bank and head of a foreign branch 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.

Internal audit of this kind should be performed in accordance with the tasks plan of the internal control and internal audit unit in a frequency determined according to an evaluation of the risk posed by individual areas of the financial institution's activity. In view of the reputational risk to the financial institution associated with unwanted involvement in money laundering or terrorist financing, it is appropriate that this thematic internal audit be performed at least once per calendar year.

Article III
Final provisions

(1) This methodological guideline replaces in full the **Methodological Guideline No 4/2009 of the Financial Market Supervision Unit of Národná banka Slovenska of 17 December 2009 regarding the prevention by banks and foreign bank branches of money laundering and terrorist financing**.

(2) This methodological guideline shall enter into force on the date of its approval by the Executive Director of the Financial Market Supervision Unit of the Národná banka Slovenska.

Ing. Vladimír Dvořáček
Executive Director of the
Financial Market Supervision Unit

ANNEX

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 signs of unusualness on the basis of information available to the financial institution's Nominated Officer at the time of assessing a transaction or other act, or on the basis of information that he can acquire within a time that does not jeopardise the reporting of an ST within the statutory period.

In assessing transactions or business relationships, it is necessary to take particular account of:

1. information from the financial institution's frontline staff on the customers and on the circumstances in which the business relationship is established or transaction executed;
2. internal reports of UTs and records on them;
3. information acquired in the framework of ongoing monitoring of the business relationship;
4. information acquired in the framework of retrospective assessment of the customer's transactions;
5. compilation reports and outputs from the financial institution's internal information system, which should contain an analytical tool for automatic evaluation and identification of signs indicating possible UTs, and which must be harmonised with the Programme. Today, given the emphasis placed on electronic banking and the quantities of transactions made daily, practically 24 hours/7 days a week, a financial institution in identifying and assessing UTs cannot work solely from information provided by frontline staff;
6. information from the financial institution's registers established under the Banking Act;
7. information received from other obliged entities;
8. information from commercial databases;
9. information from open sources;
10. information arising from requests and instructions from authorised entities, in particular the police force, prosecutor, courts, executors, etc.;
11. information from the FIU, in particular feedback on the effectiveness of UT reports received and the manner of their handling, warnings and information on indicators and new types of STs published or targeted by the FIU;
12. analyses and investigation results from AML group staff.

In analysing and assessing transactions in order to determine whether they do or do not constitute a UT, it is necessary to have particular regard to:

1. the person making or requesting the execution of the transaction or purchase of a product or service;
2. the legal person who, in the case that it does not act on its own behalf, is owned by, represented by, acted for on behalf by, or in any other way represented by such a person;
3. the customer's transaction and requests;
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., authorities;
6. decisions on the postponement of any UTs.

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

1. the customer who is a natural person, focusing particularly on:

- social status;

- age (young and old age are particular risk factors);
- nationality (in the case of foreigners identify the reasons for making transactions in Slovakia, national of a country supporting international terrorism, etc.);
- politically exposed persons;
- risk in terms 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 of 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 bureau, tax debts, debts toward the Social Insurance Agency);
- any positive record in registers of the obliged entity (ST register, rejected transactions, fraud, etc.);
- feedback and information from the FIU;
- external signs indicating affiliation to extremist groups and movements;
- documents (homeless person, a person deprived of legal capacity, suspicion of altered or falsified documents, lost documents);
- the 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 the transaction, business, etc.

2. the customer that is a legal person, focusing particularly on:

- its line of business in relation to the assessed transaction, as well as from the aspect of creating the customer's risk profile;
- whether the legal person is an obliged entity;
- the form and statute of the legal person;
- the date and place of registration from the aspect of the increased level of risk (shell companies, risk areas, etc., newly-established companies with an excessively high turnover);
- company shareholders, statutory representatives, persons authorised to act, beneficial owner – applies similarly for each legal or natural person separately;
- former company shareholders and statutory representatives;
- the course of its business to date;
- frequent changes of the company's registered address and business 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;
- any positive record in registers of the obliged entity (UT register, rejected transactions, fraud, etc.).

3. the transaction, including its form, execution method and value, focusing particularly on:

the legal and natural persons making the transaction, including:

- the plausibility of the transaction and its purpose;
- the degree of risk inherent in the transaction;
- the value and volume of the transaction;

- the subject of the transaction;
- the coverage of the transaction;
- the method and form of payment;
- documents presented by the customer;
- the customer’s requirements;
- business partners;
- information on similar transactions from open sources;
- comments on the transaction from the financial institution’s competent and professional units;
- experience with other obliged entities making the same type of transaction.

Each financial institution shall determine the forms and methods of STs 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 in the framework of the group of which it is a member.

Indicators of unusualness

Indicators of unusualness in relation to a natural person

Indications that a person may not be acting on his own behalf and may be acting under the direction of another person, i.e. a “white horse”, or that a person otherwise represents an above-average risk of money laundering and terrorist financing, include in particular that the person:

- has an unkempt appearance or poor social situation;
- appears to be under the influence of narcotics;
- is ignorant of the transaction or line of business;
- behaves in a unusual or abnormal way;
- is homeless, i.e. the person's only registered permanent residence is a local authority office, or no street name is stated in the submitted documents, or it is known by an employee of the financial institution that the person is homeless;
- owns several companies that have progressively been transferred to him over a period of time;
- is the true owner or executive of a company, but does not have usage rights for the company's accounts or never acts alone;
- is accompanied by third persons who direct or check his actions;
- uses lost, falsified or altered documents;
- intentionally submits false data, particularly on employment, place of residence, activities, etc., or refuses to respond to the financial institution’s requests;
- is sought by the police;
- is suspected of committing a crime;
- is known or suspected to be a member of a criminal group;
- is on wanted list of military or intelligence services;
- is on a list of persons subject to sanctions;
- is on a list of terrorists or sympathisers of terrorism;
- expresses through their appearance or statements sympathy to extremism;
- is a foreigner with no apparent relationship to Slovakia;
- is a foreigner from areas known to be high-risk in relation to the promotion of international terrorism;
- is deprived of legal capacity;
- is a child, youth, young adult, or elderly;

- constitutes a higher corruption risk – e.g. representatives of government or political parties;
- is a politically exposed person, foreign public official;
- represents a foundation, non-profit association, etc.;
- has been the subject of a UT report;
- is a non-payer or unreliable according to registers or other information available to the financial institution's staff;
- is 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 transaction or any act is made 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.

Indicators of unusualness in relation to a legal person

- A natural person posing an increased risk of money laundering or terrorist financing represents the legal person, owns it, or is its beneficial owner in any demonstrable relationship.
- The legal person's registered line of business is not in accordance with its real business.
- The line of business is high-risk in terms of the potential for money-laundering – in particular gambling, bureaux de change, trade in receivables, restaurant services and other operations working with cash.
- The line of business requires a special permit.
- The legal person's ownership structure is unclear.
- The legal person, owner and owner or company shareholder thereof is domiciled in a tax haven or high-risk area in terms of the support and financing of terrorism.
- The legal person has only a virtual registered office.
- The legal person is a ready-made company.
- Another obliged entity – tendency to not devote attention to the transactions of another obliged entity,
- The legal person trades with other legal persons posing a risk of money laundering or terrorist financing.
- The legal person has misleading business name or line of business, suggesting that it may be a bank, financial institution, etc.
- The legal person is a shell bank.
- The financial institution knows from available registers that the legal person is a debtor or has failed to fulfil its tax obligations.
- The legal person is known to have been misused or involved in any other way whatsoever in the commission of a crime.

Indicators of unusualness in relation to a transaction or request for its execution

1. A transaction made by natural or legal persons who represent an increased risk of money laundering or terrorist financing.

2. A 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 transaction of the particular type or particular customer, or that has no clear economic or lawful purpose.

3. A transaction in which the customer requests the establishment of a contractual relationship or execution of a transaction with the obliged entity on the basis of an unclear project.

4. A 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 transaction in which the customer submits false, invalid or stolen identification documents, forged banknotes, falsified documents or securities, etc.

6. A transaction in the case of which the customer refuses to or cannot submit supporting documentation.

7. High-value credit transfer to the customer's account followed by cash withdrawals in amounts corresponding to the maximum unreported cash withdrawal.

8. An attempt by the customer to obtain credit for financing activities unrelated to the customer's line of business.

9. The use of money transfer services provided by the financial institution, in parallel with ordinary payments, despite being disadvantageous for the customer.

10. A refusal to provide information on the basis of which under ordinary circumstances customers could obtain credit or other banking services.

11. An attempt by the customer to obtain credit where the source of the customer's financial contribution for the transaction is unclear.

12. Repeated and frequent changes to the right to use an account, made by the account holder on the basis of a power of attorney.

13. Repeated deposits by a large number of customers who make payments to the same account with no apparent purpose.

14. An attempt to perform financial transactions using various unknown guarantees and warranties.

15. The opening of accounts or performance of transactions, particularly for foreigners, by means of an authorised person.

16. The transfer of large sums of money to or from abroad using payment services.

17. A transaction in which there is a reasonable assumption that the subject of the transaction is or should be a thing or service that may relate to a thing or service upon which international sanctions have been imposed under a separate regulation.

18. Transaction made from or to a country with increased risk of terrorist financing or countries with a high security risk (drugs, weapons, etc.).

19. Fund transfers via postal orders made by a representative of a legal person in favour of an account of a different legal person or sole proprietorship.

20. The refund of an excessive deduction of VAT or other payment from a state treasury account (usually to a newly opened account not registered by the tax administrator, or unused for a long period) and its immediate withdrawal in cash or transfer to another account and its subsequent withdrawal in cash, or subsequent immediate change in the form of funds, e.g. in the form of an investment in securities, etc.

21. Transactions on a personal account that have the nature of business activity or a link to such activity, where these actions may be masking illegal income, since the customer creates the impression that it constitutes management of personal finances.

22. Growth in high account balances that are not in accordance with the customer's known and normal turnover, and their subsequent transfer to an account (or accounts) abroad,

23. A significant increase in deposits of cash or negotiable securities from the side of a legal person, with the use of accounts of a different customer or internal accounts of a company or securities accounts, in particular where the deposits are immediately transferred between a different company of the customer and the securities accounts

24. A customer's request for investment (securities) management services, where the source of funds is unknown or not consistent with the customer's apparent, in particular financial, situation,

25. Transactions involving limited liability companies in which there has been a change in the position of executive, a change of business name, change of registration court, etc.,

26. A payment from abroad, particularly a country outside the EU, with the transaction description stated as donation, aid, loan, etc. and its immediate withdrawal in cash, or immediate transfer to a different account.

27. A cash deposit to an account and subsequent request by the customer to issue a confirmation of the current account balance, followed by a withdrawal from the account.

28. Several movements on an account in one day or consecutive days, not corresponding to the customer's ordinary financial operations,

29. A cash deposit or transfer abroad, where the customer states the payment purpose as a fee or commission.

30. An unusually large 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.

Methods of money laundering or terrorist financing by UTs may include in particular those listed as follows.

1. An artificial increase in turnover in the case of firms dealing with cash. Proceeds from crime in the form of cash are mixed with proceeds from legal activity, with the result of the mixing declared as legal income and legal turnover.

2. Funds transfers from abroad to accounts of natural persons or legal persons, followed by the immediate withdrawal, or transfer of almost the whole credited amount, where there is the risk of frustrating seizure of that income for the purposes of criminal proceedings. This concerns in

particular revenues from such activities as phishing, pharming, vishing, internet fraud, payment card fraud, payment terminal fraud.

3. Depositing proceeds from crime in bank accounts in tax havens or in accounts of companies that are registered in offshore areas; the account may be set up virtually anywhere.

4. Transfers between companies with an unclear ownership structure that do not have any apparent economic basis or reason.

5. Dealing in arms and hazardous materials that are covered by fake transactions made by companies domiciled in a tax haven, with local accounts used only for transfer and for obscuring financial flows.

6. Misuse of lawyers' or notaries' customer accounts, the primary objective not being to provide services, but to create a credible source of funds.

7. Reverse loans, most often using accounts of foreign natural or legal persons, usually domiciled in a tax haven.

8. Investments by foreign entities committing crime in Slovakia and vice versa. This concerns particularly investments in real estate, securities, high-value goods and the purchase of shares in companies.

9. Payments made by non-profit organisations, non-investment funds and foundations, or in their favour, that do not correspond to the purpose of their founding.

10. The use of domestic and foreign accounts, in particular those of natural persons, for online betting and online gambling.

Types of UT include in particular those listed as follows.

A. Private Banking

1. A transaction in which the customer refuses to provide information on an intended transaction or seeks to provide as little information as possible or provides only information that the obliged entity can check only with great difficulty or at great cost.
2. A transaction in which the volume of funds that the customer has is in clear disproportion to the nature or scope of his business activity or declared financial circumstances, or where the customer's account movements do not correspond to the nature or scope of their business activity or the customer's usual financial operations.
3. A one-time cash deposit to an account that does not correspond to the customer's hitherto activities and information that the financial institution has available on the customer.
4. Frequent repetition of cash deposits for no apparent reason, through which a large deposit accrued and was then transferred to a place that under ordinary circumstances is not associated with the customer.
5. Frequent cash deposits to an account used for covering bank drafts, money transfers or for other negotiable and highly liquid cash instruments.
6. Unusually high cash deposits made by a natural or legal person in whose business activities cheques and other instruments would normally be used.
7. Client activity relating to the opening of multiple accounts, the number of which is in clear disproportion to the line of business and the related transactions between these accounts.
8. Cashless deposits by third parties and subsequent cash withdrawals of the funds by the

customer for purposes for which other forms of payment, e.g. cheques, letters of credit, bills of exchange, are normally used.

9. Frequent deposits of large quantities of low-denomination banknotes to an account.

10. The frequent exchange of large quantities of low-denomination banknotes for higher-denomination banknotes.

11. The frequent exchange of cash for other currencies (attempt to conceal the origin of the money through conversion to a different currency).

12. Transactions of a customer who promises customers unusually high returns.

13. The use of letters of credit and other forms of payment usual abroad, in cases where such forms of payment are not usual in the customer's known business activities.

14. A request for a loan against assets held by the financial institution or a third party, where the origin of those assets is not known or the assets do not correspond to the customer's situation.

15. The provision of a loan that is secured by a cash deposit in a foreign currency by a third party that is not known to the financial institution in the same scope as the customer to whom it provided the loan.

16. The securing of a loan by funds "in cash", i.e. deposited on deposit accounts, or deposits in savings books.

17. The prepayment of a loan, particularly where the origin of the funds from which the loan was prepaid by the customer is unclear or where the customer in the past had loan repayment problems.

18. Repeated back-transfers of funds to foreign banks domiciled in high-risk areas or to companies domiciled in high-risk areas.

19. The purchase and sale of securities outside the customer's normal practice without proper justification.

20. Large cash deposits through night-safe deposit services, where it is possible to avoid direct contact with staff.

21. Withdrawals of large amounts of money from a previously sleeping or inactive account, or from an account on which they had just arrived and unexpectedly high deposit.

22. Increased activity on the side of natural persons in frequent use of safe-deposit services.

23. The rental of a safe-deposit box to which multiple persons have access, and whose personnel, business or other similar connection is not known.

24. A purchase of traveller's cheques in cash and their subsequent sale to the financial institution.

25. The use of letters of credit and other forms of documentary payment by customers who had not previously used in their business activities letters of credit or other payment instruments, and who began within a certain period, without giving proper reasons, to use these payment instruments to a greater degree.

26. A large or unusual settlement of securities in cash.

27. The purchase and sale of securities without discernible purpose or under circumstances that seem unusual.

28. Any transaction with a broker where the identity of the beneficial owner or counterparty is secret, contrary to standard practice for the given type of transaction.

29. Transactions involving newly-incorporated companies registered in tax havens.

30. Repeated back-transfers of funds to foreign banks domiciled in high-risk areas and from these banks.

31. Transactions relating to acts by notaries and lawyers on behalf of customers, or a payment from abroad, outside the EU, and its withdrawal in cash and subsequent closure of the account.

32. The involvement of a firm or financial institution from a high-risk country in a transaction.

B. Retail banking (combined into universal banking)

1. A large credit transfer to the customer’s account followed by cash withdrawals in amounts corresponding to the maximum unreported cash withdrawal.
2. A cash withdrawal in an amount that does not fit the framework of the customer’s ordinary withdrawals.
3. Repeated and frequent changes to the right to use an account, made by the account holder on the basis of a power of attorney.
4. A large number of people making payments to the same account without adequate explanation.
5. Cash withdrawals immediately following receipt of a payment from a state treasury account, or transfer of such a payment to a different account with subsequent cash withdrawal.
6. The refund of an excessive deduction of VAT, usually to a newly-opened or sleeping account and its immediate withdrawal in cash.
7. Business transactions on a personal account.
8. The accumulation of substantial funds within one day or on a preceding day acquired through a combination of cashless and cash transactions.
9. The accumulation of a large balance on account which is not in accordance with the customer’s known company turnover and its subsequent transfer to an account (or accounts) abroad.
10. A payment of a commercial nature between two customers of the same branch made as two transactions, namely a cash withdrawal and subsequent cash deposit, usually without movement of the cash.
11. A customer's attempt to enter into a contractual relationship with the financial institution or perform a banking operation on the basis of unclear projects, or to set up an account with the minimum balance, with a request for a confirmation of the account balance.

C. Electronic – internet banking

1. A large credit transfer to the customer's account followed by cash withdrawals by payment card in amounts corresponding to the maximum unreported cash withdrawal.
2. The customer transferring large sums of money abroad or from abroad clearly at variance with the information that the financial institution has available.
3. A payment from abroad, particularly outside the EU, and its immediate cash withdrawal by payment card.
4. A payment from abroad, particularly outside the EU, with the purpose stated as "donation".
5. Operations made via Internet banking, where there is missing data on the payment purpose.
6. Internet lottery and gambling – an amount being credited to a player account and then transferred to a different account without any, or negligible, actual gambling.
7. Frequent changes of the telephone number for receiving the SMS code generated by the system, needed for identifying the customer in making an account transaction.
8. Funds being transferred from an account immediately after being credited there from a different account.
9. Operations made in connection with the performance of business activity (payments for goods, invoices, payments from the state treasury).
10. A notice of a change of address prior to delivery by courier of the contract on the opening of an account, as compared to the address stated when filling out the data in the contract on opening of an account online via the internet.
11. Operations made on an account where payments are in low nominal values, though in an extraordinarily high volume.
12. Frequent ATM cash withdrawals, even at the cost of increased charges for individual withdrawals.

D. Investment banking

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

E. Home savings

1. The prepayment of a loan on a home savings account, on which the customer had in the past been recorded as insolvent.
2. The repayment of instalments to a home savings account from accounts of legal or natural persons not held by the saver, or from multiple accounts.
3. The termination of a home savings account with payment of the balance to an account different from that from which regular repayment instalments were made.
4. The payment of a balance from several home savings contracts of various customers to the same account number.
5. Multiple repeated changes to a saver's account during the course of a year for regular or lump-sum payment of insurance premiums.
6. Payments to several home saving accounts of the same customer in a high volume, with the funds deposited in the account in cash.
7. The payment of saving instalments by the customer exclusively in low-denomination banknotes.
8. The payment of instalments in a lump-sum amount above €15 000 per contract.
9. The payment of saving instalments by transfer from accounts registered offshore.
10. A customer requesting that a payment erroneously sent to his home savings account be reimbursed to an account different from that from which the payment was made.