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

Národná banka Slovenska, the Financial Market Supervision Unit, (hereinafter referred to as the "NBS"), 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, Financial Intelligence Unit, in order to provide for a uniform procedure in fulfilling their duties in the area of prevention of money laundering and terrorist financing, issues this methodological guidance:

PART I

Article 1
Subject matter and purpose

(1) The purpose of this methodological guidance is to provide companies engaged in investment services and investment activities, old-age pension saving, supplementary pension saving and collective investment with explanatory material for fulfilling their duties arising under legal regulations focused on the prevention of money laundering and terrorist financing in the financial system. The legal regulation in this area is complex, as it is based not only on binding Slovak legislation, but also on international standards, knowledge, and practical experience gained in the performance of supervision and control by the NBS and the Financial Intelligence Unit, respectively.

(2) This methodological guidance also contains the specification of the way in which the NBS shall, in carrying out supervision, exercise and interpret the basic duties and tasks in this area, criteria under which it shall assess the implementation of legal provisions as well as the compliance with rules for prevention of money laundering and terrorist financing.

(3) In preparing this methodological guidance, the authors have worked from the fact that the rules laid down by the legal regulations represent minimum requirements; the authors, through this methodological guidance, neither can nor seek to give instruction for solving all cases that arise in practice. The rules do, though, give the freedom to use other sources of information and to set one's 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 guidance, it is also possible to use more sophisticated methods, particularly those already used and proven in practice.

(4) The purpose of this methodological guidance is to define, specify or explain the content of terms associated with the fulfilment of obligations in the area of prevention of money laundering and terrorist financing, and thus help create one's own Programme for combating money laundering and terrorist financing.

Article 2
Definitions

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

Investment firm	legal entity domiciled in the Slovak Republic, established as a joint stock company pursuing activity in the Slovak Republic under Article 54(1) of the AoSIS
Branch of a foreign investment firm	branch of a foreign investment firm pursuing activity in the Slovak Republic under Article 54(5) of the AoSIS
PFMC	pension funds management company whose organization and activities are governed by Act No 43/2004 Coll. on old-age pension saving
SPMC	supplementary pension management company whose organization and activities are governed by Act No 650/2004 Coll. on supplementary pension saving
MC	management company and foreign management company whose organization and activities are governed by Act No 203/2011 Coll. on collective investment
Financial institution or company	all the above mentioned financial institutions collectively – investment firm, branch of a foreign investment firm, PFMC, SPMC, MC and foreign MC
AoSIS	Act No 566//2001 Coll. on securities and investment services and on amendments to certain laws, as amended
AoOAPS	Act No 43/2004 Coll. on old-age pension saving and on amendments to certain laws, as amended
AoSPS	Act No 650/2004 Coll. on supplementary pension saving and on amendments to certain laws, as amended.
AoCI	Act No 203/2011 Coll. on collective investment, as amended
Act	Act No 297/2008 Coll. on the prevention of legalisation of proceeds from criminal activity and terrorist financing and on amendments to certain laws, as amended
AoIIS	Act No 126/2011 Coll. on the implementation of international sanctions, as amended
AML or AML area	area regulated by the Act and the AoIIS
FIU	Financial Intelligence Unit of the National Criminal Agency of the Presidium of the SR Police Force
ST	suspicious transaction
Employee	employee of a financial institution fulfilling the tasks defined by law
Legalisation	legalisation of proceeds from criminal activity
NO	nominated officer as defined in Article 20(2)(h) of the Act
KYC	“Know Your Customer” principle
FATF	Financial Action Task Force (a leading institution in determining international standards to combat money laundering and terrorist financing at the global level)

Article 3
"Dirty" money and legalisation

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

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

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

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

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

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

(3) All financial institutions whose activity is regulated by this methodological guidance are, in the course of their business, exposed to the risk that their clients 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.

PART II

Prevention of money laundering and terrorist financing within the financial institution's activity

Article 4
Policy of protection 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 the "AML/CFT Policy"). The AML/CFT Policy must be set so as to ensure effective performance of activities aimed at preventing and detecting money laundering and terrorist financing 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 guidance by Slovak and foreign regulators, analyses by major Slovak and foreign institutions or consultancy firms, and last but not least the experience and the approach of other companies. In creating the AML/CFT Policy, an investment firm shall take into account its business objectives, the existing clientele, the range of provided services, the method of providing the services in relation to the individual financial instruments, 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 system, with particular relevance to operational risk management.

(4) The statutory body of the financial institution is responsible for the financial institution's overall AML/CFT prevention.

(5) Responsibility for the practical implementation of activities in the field of AML/CFT, primarily the performance of day-to-day activities ensuring the implementation of the AML/CFT Policy, lies with the nominated officer.

(6) Responsibility for the overall protection of the branch of a foreign investment firm lies with the head of the branch of a foreign investment firm or other responsible person (hereinafter referred to as the "Branch's Responsible Person"). The AML/CFT Policy at the branch of a foreign investment firm is adopted and implemented by the branch's responsible person.

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

Article 5
Employees responsible for implementing AML/CFT tasks

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

(2) The branch's responsible person is responsible for the overall AML/CFT prevention at the branch of a foreign investment firm and for implementing the AML/CFT Policy.

(3) Responsibility for the practical implementation of AML activities, primarily the performance of day-to-day activities ensuring the implementation of the AML/CFT Policy, the reporting of suspicious transactions, and ongoing contact with the Financial Intelligence Unit in the financial institution lies with the NO.

(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, taking into account its personnel capacities, the size and range of the provided services.

(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, depending on the provided services and performed activities.

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

(8) The NO of the branch of a foreign investment firm is appointed and dismissed by the responsible person or the head of the branch a foreign investment firm. The NO of the branch of a foreign investment firm reports to the responsible person of the branch or to the head of the branch a foreign investment firm.

(9) The NO shall be responsible mainly for:

a) ongoing preparation and updating of the Programme and any other necessary regulations and procedures for the AML field,
b) fulfilment of management and control tasks in the field that he performs and for which he is responsible,
c) communication, cooperation and maintaining ongoing contacts with the Financial Intelligence Unit, including the timely reporting of STs,
d) organisation and setting of rules for the training of the relevant staff, including new staff,
e) analytical and advisory activity in relation to the assessment and reporting of STs by the respective staff in connection with the execution of clients' transactions and financial operations.

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

(11) The NO shall prepare and submit a report on his activity to the statutory body at least once a year. The NO of the branch of a foreign investment firm shall prepare and submit a report on his activity to the responsible person of the branch and to the head of the branch of a foreign investment firm at least once a year.

(12) The activity report of the NO shall contain in particular the following information:
a) statistics and a brief description of STs reported by staff,
b) statistics and a brief description of STs reported by staff that were not forwarded to the FIU, with reasoning,
c) statistics and a brief description of STs forwarded 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 the AML/CFT Policy is to ensure that the NO and his deputy 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 and his deputy:

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 clients' transactions and financial operations,
c) unlimited access of the NO and his deputy to all documents, databases and information at the financial institution,
d) autonomous and independent decision-making of the NO and his deputy in assessing the suspiciousness of clients' transactions reported by the respective staff in the framework of the internal reporting system,
e) autonomous and independent decision-making on the sending of ST reports to the FIU,
f) control function of the NO and his deputy in relation to units and staff responsible for executing clients' 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), which means that the function of the NO and his deputy must not coincide with the function of the financial institution's internal controller, but the accumulation of powers in the compliance function or in other functions is not exempted,
h) cooperation with the compliance and internal audit staff in the new types of transactions; 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,
and the appropriate definition of the position of the NO and his deputy specified in points (g) and (h) shall be made in proportion to the size of the financial institution, nature, extent and complexity of the provided services and performed activities and to the actually established functions.

Article 6
Programme of own AML/CFT activity

(1) A financial institution shall draw up the Programme of own AML/CFT activity (hereinafter referred to as the "Programme") as an internal regulation to be approved by the statutory body. The Programme shall be based on generally binding legal regulations, in particular the Act, the AoSIS, other applicable laws, methodological guidance of the FIU published and regularly updated on the website of the FIU (http://www.minv.sk/?aplikacia), as well as on international standards – 40 FATF Recommendations.

(2) The Programme shall also take into account the financial institution's AML/CFT Policy and 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 and relevant staff of the

financial institution in the performance of activities, types of transactions and financial operations of clients in terms of statutory requirements (in particular Article 20(2) of the Act) for the AML/CFT prevention, as well as the control powers of such entities and control powers of the compliance and internal audit staff. 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 clients' transactions and financial operations, as well as the most common forms of STs at the given financial institution. 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 activities and services, the types of transactions in relation to the individual financial instruments and their range and specifics, the type and number of clients, and the specifics and range of such clients' operations.

(4) In addition to the general elements defined in Article 20 of the Act, the Programme shall contain in particular:

a) the exact specification of responsibilities and related competences arising from comprehensive AML/CFT prevention at the individual levels of management from the board of directors of the financial institution, or from the responsible person of the branch of a foreign investment firm down to the units of first contact with the client, including the Prevention Unit, with the definition of the NO pursuant to Article 20(2)(h) of the Act,
b) the nomination of the NO pursuant to Article 20(2)(h) of the Act,
c) the specification of person (persons, where appropriate) responsible for assessing whether an imminent or ongoing transaction is suspicious, the specification of the time when the assessment is to be performed (where possible, always before the execution of a transaction or in the process of its preparation), the specification of the method of performing assessment, i.e. to state what needs to be performed in an assessment, what aids are to be used (e.g. an overview of the forms of STs, publicly available information on debtors and defaulters, internal lists of clients, etc.), how and where to record the assessment result,
e) the exact specification of the procedure for receipt of notifications on identified STs from organisational units, the evaluation of these notifications and the reporting of STs to the FIU, and arrangements ensuring ongoing working contact with the FIU, or law-enforcement bodies,
f) the specification of basic tasks of the respective staff at all levels of management, the detection of STs and the reporting of internal notifications of STs to the NO (possibly also a specimen form for internal notifications of a ST), and the manner of ensuring the protection of the respective staff in connection with the ST they identified and reported to the NO,
g) the duty to identify clients in executing transactions and individual financial operations and the duty to verify such identification,
h) the duty to record the identification made and the verification of client's identification, as well as all financial operations executed for the clients,
i) the obligation to retain records on the client identification and on the verification of their identification and on the financial operations conducted by the clients, and this for the period set by the Act,
j) an overview of known, already detected types of STs, broken down by activity and type of transaction executed,
k) the evaluation and management of risks associated with money laundering and terrorist financing, including client assessment procedures based on a risk-oriented approach and risk analyses, taking account of the results of initial and ongoing client identification and verification of their identification, broken down by type of transaction and type of operation and account,

l) the specification of the method and extent of the implementation of customer due diligence on the basis of risk evaluation results pursuant to Article 10(4) of the Act,
m) detailed signs of suspiciousness by which a client's STs can be recognised,
o) the manner and scope of feedback at the financial institution on internal notifications of STs
o) the procedure of the competent staff and NO in delaying a suspicious transaction under Article 16 of the Act,
p) the content and timetable of staff training, training staff for performing AML/CFT tasks in the performance of particular banking activities, types of client transactions and operations,
r) the duty to maintain confidentiality regarding an internal notification of a ST and its reporting to the FIU and regarding measures performed by the FIU (Article 18 of the Act), primarily in relation to the client concerned, as well as toward persons having a certain relationship to the client (e.g. other authorised users of the client'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,
r) measures and control mechanisms preventing the abuse of position or function by the relevant staff to knowingly engage in money laundering or terrorist financing in the exercise of their function;
s) the method and periods for retaining data and documentation,
t) 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,
u) definition of information flows and description of information systems focused on the collection, processing and reporting of information for the purpose of AML/CFT, including regular reports submitted to the board of directors and supervisory board of the financial institution and to the 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 internal 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.

Article 7
Staff awareness and training

(1) The persons responsible for the AML area in the financial institutions must be aware that the actual assisting, a client's knowing or unwitting involvement in money laundering or terrorist financing represents an operational risk. The financial institution can ultimately suffer significant financial losses if it executes operations using the proceeds or instruments from any criminal activity, whilst its reputation may also suffer (reputational risk).

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

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

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

(6) The financial institution, in informing and training staff, shall take account of its conditions, in particular its size and organisational arrangement, activities and types of transactions and financial operations performed for clients, so that all necessary information reaches all staff for whom the information is intended. The model for performing staff training is to be effective, flexible and fulfil the desired objective; therefore it is essential that it be updated with regard to changing conditions.

(6) The effectiveness of a financial institution's AML/CFT prevention 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 the performed investment services and activities, incidental services and types of transactions and, in particular, the diversity in the structure of clients 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 client) must have all necessary information on the performed investment services and activities, incidental services and types of transactions they execute for clients, and they must learn as soon as possible the criteria (signs of suspiciousness) for assessing, or detecting, STs. These staff must be able to assess the conduct of the financial institution's clients, as well as the content of financial operations performed by clients in terms of their degree of risk, unusualness or suspiciousness. Staff training should significantly contribute to staff acquiring the necessary skills to master procedures for applying the Know Your Customer principle (hereinafter referred to as "KYC") and to recognise the degree of risk from actions of the financial institution's clients, also with regard to the client'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 client's STs.

(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 with the consequences of a breach of the prohibition of providing a client 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 ST.

(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 provision 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. Each competent employee who performs tasks under the Act must be familiarised with the applicable Programme governing procedures in

assessing clients and their financial operations, and concurrently the financial institution is required to ensure that each employee has permanent access to the Programme.

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

(10) Specialised training that the financial institution's staff should complete before they process clients' instructions for the execution of financial operations should give them the necessary knowledge for ascertaining and verifying a client'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 client's commercial activities from their related financial operations, and, therefore, also the necessary knowledge and capability to identify facts outside the client's expected behaviour, and specific manifestations of their STs.

(11) A financial institution should repeat and supplement training with new knowledge, where necessary, also more frequently than in a 12-month cycle, so as to ensure that the relevant staff are able to continuously perform their duties. 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 8
Information system

(1) A systematic approach to the financial institution's risk management and AML/CFT requires mainly the creation of appropriate information flows for ensuring the smooth, timely and regular flow of information between individual levels of management at the financial institution, including its statutory body, the NO, the deputy NO, the compliance and internal audit staff, and other relevant staff. 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.

(2) In addition to the information systems including application software for ensuring information flows for the system of AML/CFT, the financial institution may for support, and depending on the number of business transactions and instructions, use a specialised automated system for detection of STs and persons subject to sanctions in the financial institution's relevant information systems, which operates on the basis of set scenarios on databases of clients, transactions or financial operations.

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

a) transmission of information to staff on AML/CFT principles, procedures, duties and related powers for performance of tasks in the given area,
b) making the Programme and other relevant internal regulations available to all employees,
c) transmission of necessary information between the responsible person and the NO,
d) transmission of information between staff and the NO and vice versa, including the internal reporting of STs,
e) record-keeping, i.e. the recording, processing and updating of data on clients and the recording and monitoring of clients' transactions,
f) communicating to the statutory body or responsible person the results of control performed by the NO and compliance and internal audit staff, as well as informing staff of these results,
g) transfer of information between the NO and the FIU, including the reporting of STs 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 STs in the financial institution's relevant information systems that contain data on clients and their operations.

(4) The form, content and rules of information flows should be set by the financial institution depending on its size, focus, scope and complexity of its activities and on the types of transactions and services offered by it, as well as on the characteristics of its clients 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.

(5) An essential component of a financial institution's information system is an electronic information system (hereinafter referred to as an "EIS") that complies with statutory requirements, with the aim of ensuring a sufficient quality of AML/CFT prevention. It is a system recording and processing data on clients and their financial operations which must take account of the requirements provided for in Article 9(e) of the Act:
a) in the case of a natural-person client, the EIS must contain records of at least the name, surname, date of birth or birth registration number and the client's account numbers, and in the case of a natural-person entrepreneurs also the identification number, if assigned,
b) in the case of a legal-person client, the EIS must contain records containing at least the client's name (trade name) and identification number.

The EIS must also contain information or records on the nature of the client's business relationship which 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 service used by the client. The EIS and the manner of using it should make it possible to identify STs performed by clients, and, as relevant, monitor also their course or development, as well as the connections between the financial operations of a certain client and, where possible, also the suspicious transactions of different clients.

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.

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), and it should also be capable of providing in a timely manner and sufficient scope data to the FIU, the NBS as the supervisory authority and law enforcement authority in cases specified by the Act.

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

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

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

(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 € 2,000. It shall observe the duty to ascertain whether the client is acting on their own behalf. For the purposes of this methodological guidance the "execution of a transaction on the client's own account" or with their "own funds" should be understood as the client 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 73(5) of AoSIS (by analogy Article 55(3) of AoCI), 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, in an appropriate scope also verifying, the beneficial owner is governed primarily by the provisions of Articles 9 and 10 of the Act. 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 in 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 client'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 public sources, without the need to contact the client or verify this information with the client.

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

For illustrating possible situations in determining the client's beneficial owner in the case of legal persons there is given an overview of practical procedures used in EU Member States, which are listed in the material drawn up and published in April 2012 in the Anti-Money Laundering Committee (AMLC) operating in the Joint Committee of the 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 client, terminate an existing business relationship with a client, or refuse to perform a specific transaction in the case where it is not possible to perform basic customer due diligence under Article 10(1)(a) to (c) of the Act through the fault of the client.

A comparable duty arises also under Article 73(3) of the AoSIS. 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 guidance 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 clients, the client acceptance process should include basic customer due diligence, as well as the client'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 client's expected transactions and any foreseeable scheme of operations to be performed by the client. Based on this it is possible to create the client's risk profile. The main factors in the creation of the client's risk profile include particularly the criteria such as the purpose pursued by the client when entering into a business relationship, the type and origin of the client, its geographical residence, geographical area of the client's business activities, the nature of business activities, the source of capital (funds), the source of funds (wealth), the frequency and scope of the client's activities, the type and complexity of its business relationships.

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

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

(8) By means of categorising clients according to their risk profile the financial institution can then in practice apply Article 10(1)(d) of the Act - ongoing monitoring of the business relationship, which leads to recognition and subsequent reporting of STs. In connection with the risk categorisation of clients, 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 client's 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 its Programme of own activity.

(9) Subject to Article 9(e) of the Act, the client shall mean the person that is a party to the obligation relationship associated with the obliged entity's business activity. The portfolio management being one of the provided investment services of the investment firm within the meaning of Article 6(1)(d) of the AoSIS, it is necessary that the investment firm takes all measures in managing the portfolio of the client's financial instruments for identification of the client and fulfilment of other obligations arising from its relationship with the client (customer due diligence, KYC, or reporting of ST) also in respect of persons that are a counterparty in a transaction. This

shall not apply to transactions carried out on a regulated market or in a multilateral trading system within anonymous trading.

In connection with the consideration of risk in assessing a financial institution's clients, it is appropriate to use materials prepared by experts of the Financial Action Task Force (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) :FATF Public Statement (http://www.fatf-gafi.org/topics/high-riskandnon cooperativejurisdictions/documents/fatfpublicstatement-19october2012.html); i.e. the "black list",
b) Improving global AML/CFT compliance on-going process available on the website (http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/documents/improvingglobalamlcftcomplianceon-goingprocess-19october2012.html); i.e. the "grey list",
c) valid conclusions from FATF monitoring available on the website of the FIU (http://www.minv.sk/?vyhlasenia-fatf),
d) the formal publication on a Member State, confirming that the country does not comply with the basic reference documents for appropriate prevention of money laundering and terrorist financing, available on the website (http://www.coe.int/t/dghl/monitoring/moneyval/),
e) currently valid conclusions from monitoring are published also on the website of the FIU (http://www.minv.sk/?moneyval-vyhlasenia),
f) detailed evaluation reports on each Member State and its system of prevention and repression in the field of money laundering and terrorist financing (in the form of a "Mutual Evaluation Report"), available in English on the website (http://www.fatf-gafi.org/topics/mutualevaluations/ and http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/Evaluation_reports_en.asp),
g) the list of equivalent third countries, which was created on the basis of agreement of the EU Member States in the European Commission Committee ("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).

(10) 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 client also in other situations, according to the client's risk profile or according to the degree of risk inherent in the service or type of transaction provided to the client (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.).

(11) 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.

(12) Where the client poses a high risk, this requires more detailed assessment of the client, the client's behaviour and orders given by the client 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. It shall also pay particular attention to selected groups of entities, in addition to the already mentioned politically exposed persons (Article 6, Article 10 and Article 12 of the Act), particularly asset pools (Article 25(2) of the Act) and shell banks (Article 24(1) of the Act).

In the case of identifying politically exposed persons, financial institutions are recommended, in accordance with the new FATF international standards published in February 2012 on the website (http://www.fatf-gafi.org/topics/fatfrecommendations/documents/fatfrecommendations2012.html) to exercise enhanced customer due diligence not just to the sphere of persons referred to in Article 6(1) of the Act, but also to persons with permanent residence in the Slovak Republic. In the process of the identification and verification of politically exposed persons it is recommended to use the existing commercial databases of high-risk clients, e.g.: World-Check database of high risk individuals and companies; website (http://www.world-check.com/). In monitoring existing clients it is essential to focus also on the ongoing monitoring and verification as to whether the client has become a politically exposed person; in such a case the consent of a managing employee, meaning an employee one management level higher, must be required for continuing the business relationship. Where a politically exposed person owns or works in the managing structure of a client – 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 client – legal person.

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

A financial institution shall apply enhanced customer due diligence also if it is preparing to establish a new business relationship or open an account without the client being physically present.

(12) 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. compliance by third parties, other than for 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, it is possible to rely on already-performed identification and verification of the client 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 client 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 compliance approach. In such cases, in accordance with the practice in EEA member countries, it is not necessary to specifically require the client's consent to the provision of data to a third party.

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

(11) A financial institution can exploit the possibility of applying a less demanding procedure in client identification, i.e. simplified customer due diligence (Article 11 of the Act). The use of simplified customer due diligence in no way represents an exemption from the duty to monitor the business relationship on an ongoing basis (Article 10(1)(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. Simplified customer due diligence of the obliged entity shall mean the identification of the client, where no verification of such identification is required.

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 the fact that a particular client 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 10
Detection, reporting and delay of STs

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

Under Article 14(1) of the Act the financial institution is required to assess whether an imminent or ongoing transaction is suspicious. Under Article 20(1) and (2)(d) of the Act, the 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 STs), 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) A ST is a legal act or other act that indicates that its execution may lead to money laundering or terrorist financing (Article 4 of the Act). Article 4(2) of the Act gives a demonstrative calculation of a ST. There are several signs (indicators) of suspiciousness (e.g. an unusually high volume of funds with regard to the type of transaction, an unusually high volume of funds without clear economic or legal purpose, etc.) that the financial institution is required to assess, identify, evaluate and concurrently apply the KYC principle (the Act does not define any KYC principles, though where an obliged entity applies them in practice, it is necessary to thus define them in the Programme).

Only by such action can it competently assess whether a client's imminent or ongoing transaction is or is not suspicious. 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 ST. The decisive element for assessing the client's transactions is the application of the KYC principle and the proper recognition of indicators of suspiciousness, 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 clients, in the framework of drawing up an overview of the forms of ST (Article 20(2)(a) of the Act). Based on practical experience of supervisions exercised by the competent bodies, the following transactions can be considered a ST within the assessment of all identifiers of suspiciousness: execution of transaction (purchase – sale of securities) by an agent who is an identical person in the case of both the transferee of securities and the original holder of securities, transfer of shares of a company that was declared bankrupt, with the transferor and the transferee being an identical person (member of the board of directors), arrangement of deals with securities from a risk country, transfer of funds for arrangement of deals from an account other than that specified by the client without apparent reason or explanation, the client having permanent residence in an offshore country (tax heaven), as well as a ST within the specific regulation of the old-age and supplementary pension saving – it can be the payment of a contribution to the old-age or supplementary pension saving scheme which deviates from the usual

payments by the client as for the amount or unusual frequency.

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

Such procedure enables a financial institution to satisfy itself adequately as to the actual identity of each client and identify the purpose and planned nature of commercial activities that a client will probably conduct. This procedure is also the starting point for a financial institution in determining the client's risk profile, determining the degree of customer due diligence pursuant to Article 10(4) of the Act, and accepting a client. 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) A financial institution is required, in applying each type of customer due diligence, to assess whether an imminent or ongoing transaction is suspicious (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 or legal purpose, and to make an appropriate record on them, i.e. internal reporting of a ST (Article 14(3) of the Act), which needs to be archived for the period prescribed by law.

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

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

The assessment of a client's transactions is performed by staff of the financial institution who, in fulfilling their duties, are in contact with the client, particularly those staff who receive or process a client's instructions for execution of the client's transactions or financial operations, or superiors of such staff. 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 ST can be delayed and promptly reported.

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 client and to know the purpose and planned nature of the commercial activities that the client will probably perform. This procedure is also the starting point for the financial institution in accepting a client, determining the client's risk profile, and determining the degree of customer due diligence pursuant to Article 10(4) of the Act.

A crucial element for assessing a client's transactions is here also the appropriate application of the KYC principle and its procedures and skilled identification of signs of suspiciousness. This procedure enables the employee to assess a client's imminent or ongoing transactions by comparing them against an overview of forms of STs (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 client and its otherwise usual transactions.

If an employee judges an imminent or ongoing transaction to be suspicious, 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 referred to as the "Notification of a ST").

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 client's transactions also in the framework of ongoing monitoring of the business relationship.

The assessment of imminent and 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 client may also be known to the financial institution where the client has already executed several occasional transactions (Article 10(2)(b), or (c) of the Act). This, therefore, is not the first contact with the client and the financial institution may take account of the client's existing risk profile and history of transactions performed by the client.

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 client'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 client 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 some of the signs of suspiciousness of clients' 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 clients. The set criteria or limits defined by the financial institution for this purpose must be regularly verified so that it is possible to determine their adequacy in regard to the identified levels of risk. The financial institution is also required to regularly review the adequacy of the existing system and individual processes of protection and prevention.

For assessing transactions, importance shall be given, in the framework of ongoing monitoring of the business relationship, to imminent or ongoing transactions of a client that do not correspond to the client's known or expected activity or to the forms of STs referred to in the Act or specified in more detail in the Programme. Such transactions of a client shall form the subject of assessment (Article 14(2) of the Act) and it is necessary to make a written record on 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 forms of STs, reach the conclusion that in the given case it does not constitute a ST. If this is not possible solely on the basis of information on the client that the financial institution already has available, it may, according to circumstances, request other necessary information and documents from the client 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 client's transactions that do not correspond to the client's risk profile or to its known or expected activities, it is sufficient that these operations merely indicate the fact that their execution may constitute money laundering or terrorist financing, and the NO is required to report the ST to the FIU (Article 17 of the Act).

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

c) assessment of transactions in the framework of subsequent or retrospective assessment of a

client's transactions

A means of subsequent monitoring of clients' 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 client's instructions and operations, as well as in the framework of an inspection performed by the NO.

(6) Recommended procedure in the processing and handling of internal notifications of STs and ST reports:

a) all internal notifications of STs 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 NO may not be subject to the prior consent of any person (e.g. superior),
c) the NO shall register and archive notifications on internal notifications of STs, including the position, name, surname, branch or unit of the financial institution and all data on the given client and transaction in accordance with Article 19 of the Act,
d) the NO, as well as staff of the financial institution, including its managers (members of the statutory body) involved in assessing transactions under Article 14 of the Act are required to maintain confidentiality on the notified and reported STs and on measures taken by the FIU, 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 SR 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 (c) of the Act,
e) the financial institution is required to draw up a procedure covering the period from the moment of detecting a ST through to prompt reporting of the ST, including the procedure and responsibility of staff who assess the transaction,
f) the NO, after receiving an internal notification of a ST, may confirm receipt of the notification on the ST to the member of staff who sent the notification. The confirmation should contain an instruction on the duty to maintain confidentiality under the Act. Where the financial institution has an electronic system of gathering internal reports that enables the competent member of staff to monitor the status or receipt of a submitted internal report of a ST 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 ST, or the conduct of a client, and 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 forms of STs decide whether it does or does not constitute a ST. 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 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 client that the financial institution already has available, it may, according to circumstances, request other necessary information and documents from the client pursuant to Article 10(5) of the Act. Where the NO reaches the justified conclusion that in the case of an internally notified ST it does not actually constitute a ST, the NO is required to continue documenting this decision in writing and archiving 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

ST, it is sufficient that the transaction or financial operation indicates that its execution may constitute money laundering or terrorist financing, and the NO is required to report the ST to the FIU

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

A ST may be reported in writing, electronically or by telephone (in this case it is necessary to report the ST within a period of 3 days also in person, in writing or by e-mail). The specimen form for reporting a ST, issued by the FIU, is given on the website (http://www.minv.sk/?vzory).

A ST report may be supplemented at the financial institution's own initiative within 30 days at the latest. After this period it is necessary to additionally report information and documentation acquired as another ST. In this subsequent ST the financial institution shall specify the ST to which the additionally acquired information and documentation relate.

In connection with the reporting of STs 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 unambiguous identification and verification. Only in this way is it possible to avoid security risks connected with the reporting of STs by post, fax and e-mail.

(7) The financial institutions are allowed, under defined justified conditions, to exchange information where this is related to the threat of money laundering or terrorist financing, and where it helps the obliged entities assess a client's transactions more effectively as well as alert other obliged entities to identified risks. An exchange of information may not contain the full scope of the reported ST 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.

(8) The financial institution is required to delay a ST, i.e. the execution of a transaction (Article 9(h) of the Act) as per the client's instructions, until the time of its reporting to the FIU, whilst account shall always be taken of the operating and technical possibilities, as well as of the moment when the transaction was or should have been assessed as suspicious; e.g. a client's transaction assessed in the framework of ex-post or retrospective assessment of the client's transactions can no longer be delayed. The financial institution is required under the Act to delay a ST in the following cases:

a) at its own discretion if execution of the ST 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,

b) upon written request of the FIU; the reason for delaying a ST from the side of the FIU shall always be stated in the written request.

(9) The financial institution shall not delay a ST if it is unable to do so for operating or technical reasons (it shall immediately notify the FIU of this fact), or if delaying the ST could, according to a previous notice from the FIU, frustrate the processing of the ST.

(10) The period of delaying an operation assessed as suspicious shall be at most 48 hours (Article 16 of the Act); therefore, if during this period the FIU notifies the financial institution that it has forwarded the case to the law enforcement authority, the financial institution is required to extend the period of delay, though at most by a further 24 hours. The total duration of delaying a ST is, therefore, at most 72 hours. In the case that during the time of delaying an operation the financial institution receives no instruction to seize funds from the side of a judge or prosecutor pursuant to Article 95 or 96 of Act No 301/2005 Coll. the Code of Criminal Procedure, as amended (hereinafter referred to as the "Code of Criminal Procedure"), the financial institution shall execute the delayed operation following the expiry of the set period. Prior to the expiry of the delay period, the financial institution may execute the operation only in the case that the FIU notifies it in writing that from the aspect of processing the ST, its further delay is not necessary. Saturday and bank holidays shall not be counted in the period of delaying a ST.

The start of the period of delaying an operation pursuant to Article 16 of the Act shall be deemed the moment when the client expresses the intention (will) to handle funds on its account. In the case that the financial institution presumes that the client will express an intention to execute a ST (handle funds) in the future, it is required to take personnel, organisational and technical measures so as to ensure that in case the client does give such instruction, it is not executed and thereby any potential delay of the ST is not frustrated.

The beginning of the period of delaying an operation pursuant to Article 16 of the Act may not be deemed the moment when the financial institution evaluated already-executed transactions as suspicious, or learnt of the client's executed operations. Likewise, the reason for delaying a transaction may not be the fact that the client requested from the financial institution general information regarding an account (information on the current balance of account, etc.).

Article 11
Measures against terrorist financing

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

The AoIIS 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.

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

(2) Procedure of the financial institutions in fulfilling their counter-terrorist financing obligation in the form of reporting duty:

a) financial institutions shall, in the framework of CFT, apply toward clients procedures analogous to those applied in AML, including the reporting of STs connected with terrorist financing,
b) financial institutions are required to report STs to the FIU promptly (Article 17(1) of the Act); the Act defines STs as, inter alia, a transaction in which there is a justified assumption that the client or beneficial owner is a person against whom international sanctions have been imposed, or as a transaction in which there is a reasonable assumption that the subject of it is or should be a thing or service that may relate to a thing or service against which sanctions are imposed under the AoIIS.

(3) Based on individual regulations and decisions of the European Union (hereinafter referred to as the "EU") to which lists of persons subject to sanctions (natural persons and legal persons) are attached, the financial institutions of all EU Member States are committed 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 EC. 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).

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

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

a) sanction resolutions of the UN Security Council

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

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

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

b) autonomous sanctions adopted by the EU

The EU Common Position 2001/931/CFSP as amended by Common Position 2008/586/CFSP published a list of persons subject to sanctions (natural persons and legal persons) associated with terrorism and against whom it is necessary to apply sanctions in the fight against terrorism. Persons listed in the 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 the so-called 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 the so-called enhanced judicial and police cooperation on the basis of Article 4 of the EU Common Position 2001/931/CFSP, 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 decree of the Government of the Slovak Republic

Persons included in the list of the EU Common Position 2008/586/CFSP, marked with an "*" are, however, terrorists, and on the basis of the 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 AoIIS. 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 SR Government Decree No 397/2005 Coll. declaring international sanctions ensuring international peace and security, as amended by Government Decree 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 the SR Government Decree No 397/2005 Coll. or in the relevant EU regulations governing restrictive measures.

Article 12
Archiving of data and documentation

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

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

(3) The financial institution shall store (archive) data on the identification of clients and on the verification of identification, records on clients' 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 the financial institution is required to archive for the period of five years:
a) from the end of the contractual relationship with a client, 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 executed transaction.

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

(6) The financial institution is required to archive this data and written documents also for longer than five years if the FIU requests it do so by way of a written request containing the period and scope of archiving data and written documents. This duty 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 financial institution's procedure 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 client identification and records on the client's transaction, including written records under Article 14(3) of the Act, and data on identification of the beneficial owner),
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 client,
2. the execution of a transaction with the client, 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 clients' risk rating

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

2. records on financial operations

Internal regulations of the financial institution should establish the duty to record all financial operations made for clients 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 authorities, control authorities and law enforcement authorities to compile a satisfactory record and to verify each client's risk profile. Supporting records shall contain the client's instructions related to the client's payments.

The financial institution shall archive records on each financial operation made by the client, including single financial operations performed for clients 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 STs and ST reports

The financial institution shall archive all reports on the client's suspicious activities, namely internal notifications of STs intended for the NO, as well as ST reports that the NO sent to the FIU.

If the NO, after assessing the relevant information and knowledge concerning a client's suspicious activity, decided that it did not constitute a ST 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 with 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 clients and clients' 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 clients and their financial operations in the case of which an investigation has been started from the side of law enforcement authorities, or a criminal prosecution begun, and for the purposes of investigation and criminal prosecution, on the basis of a written request by the FIU pursuant to Article 19(3) of the Act, in the scope and for the period stated in the request.

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

(8) Records prepared and archived by the financial institution shall satisfy statutory requirements for record keeping on client 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 client,

c) identification and location of each client,

d) identification of all internal notifications of STs and external ST reports,

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

Article 13
Securing the system and ensuring performance of internal control

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

(1) The system of control shall comprise a specification of control responsibilities at all levels of the management and performance of all licensed financial activities, as well as the performance of control activity by:
a) the financial institution's supervisory board,
b) members of the financial institution's statutory body,
c) nominated officer (his deputy and Prevention Unit),
d) managerial staff,
e) staff involved in the processing clients' instructions (financial operations),
f) compliance and internal audit staff who shall be responsible for controlling all units, including the NO and relevant staff.

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

It 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 financial institution and the responsible person of a branch shall regularly, at least once a year, evaluate the effectiveness of the existing system – the AML/CFT concept, 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

It 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's working procedures as well as their work duties, tasks and responsibilities in first contact with clients, as arise from AML/CFT.

f) internal control and internal audit

The compliance and internal audit staff shall control 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, or process instructions for clients' 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. performance of the relevant degrees (levels) of customer due diligence,
2. procedures for ensuring that client information received is up to date (verification),
3. assessment of specific financial operations, monitoring of clients, their financial operations and business relationships,

4. risk evaluation and management,
5. internal notification of STs and reporting of STs to the Financial Intelligence Unit,
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 financial institution should be regularly informed of the results of controls and audits performed, e.g. once a year and immediately in the case of finding serious deficiencies. 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.

PART III

Special provisions for activities of management companies

Article 14

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

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

Article 15
Duties of management company under depositary contract

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

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

PART IV

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

Article 16

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

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

Article 17
Final provision

This methodological guidance 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