Methodological guidance of the Financial Market Supervision Unit of the National Bank of Slovakia of 17 December 2009 No. 4/2009 for protection of a bank and branch office of a foreign bank against money laundering and terrorist financing

By virtue of Art. 1 (3) a) 3. of Act No. 747/2004 Coll. on financial market supervision, as amended, the National Bank of Slovakia, the Financial Market Supervision Unit, issues the following guidance in collaboration with the Ministry of the Interior of the Slovak Republic, the Financial Police Intelligence Unit and the Ministry of Finance of the Slovak Republic.

PURPOSE AND CONTENT

Banks and branches of foreign banks (hereinafter collectively referred to as a „bank“) are exposed to the risk that customers will misuse their services in the process of legalization of income gained by means of criminal activity (hereinafter referred to as „money laundering“) or for terrorist financing. Financial losses are impending over banks, if they neglect the identification and assessment of their customers, do not detect unusual financial operations of customers, or their employees help the customers to misuse the bank for money laundering, for terrorist financing or for fraud. If the bank gets into connection with money laundering or terrorist financing due to insufficient prudence in the conduct of banking activities, it will suffer a loss of credit as a result of negative publicity, and thereby also a loss of confidence of the public and an economic loss, which can cause a loss of confidence of the public in other banking entities and an impairment of the stability of the banking system.

Integrity and honesty of the management and its resolve to prevent that the bank is used for money laundering or terrorist financing, are primary protection against such efforts. Bank managers not only must have a concept for protection against money laundering and terrorist financing, but they also must put through effective measures, which ensure particularly

- the ascertainment (hereinafter referred to as „identification“) and verification (hereinafter referred to as „verification“) of the actual identity of customers – persons entering into business relationships with the bank,
- the detection and rejection of customers and operations that are unusual, and
- the necessary cooperation with police bodies and supervisory authorities, the public prosecutor‘s office and courts.

As of 1 September 2008, banks are obliged to comply with duties and apply rights focusing on the prevention of money laundering and terrorist financing in the banking system, as regulated by Act No. 297/2008 Coll. on the prevention of money laundering and terrorist financing and on amendments to certain acts (hereinafter referred to as the “Act”) and, at

the same time, to proceed in accordance with the provisions of Act No. 483/2001 Coll. on banks and on amendments to certain acts as amended (hereinafter referred to as the "AOB").
The duties and rights regulated by the Act result from the implementation of Directive No. 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (hereinafter referred to as the "third directive"), adopted in June 2005, published on 26 October 2005 in the Official Journal of the European Union and effective from 15 December 2005. The details and implementing measures for the third directive are regulated by Directive 2006/70/EC laying down the definition and technical aspects of politically exposed persons and the technical criteria for simplified diligence.

The purpose of this methodological guidance is to provide banks with explanatory material for the fulfilment of their tasks resulting from the provisions of the Act and the AOB and focusing on the prevention of money laundering and terrorist financing in the financial system, by which forty recommendations of June 2003 and nine special recommendations of the Financial Action Task Force (in addition to duties resulting from EU Regulation No. 1781/2006 on information on the payer accompanying transfers of funds) and the special recommendation VII) have been taken over.
Duties laid down by the above mentioned laws are the minimum requirements imposed on banks in their protection against money laundering and protection against terrorist financing. However, in accordance with the purpose pursued by the Act and by this methodological guidance, banks can use also more advanced and stringent procedures, particularly procedures that are already in general use and time-tested in their practice or in the practice of their parent companies from other member states of the European union, so that they can contribute in a better way to the implementation of a global policy of prevention and protection against money laundering and terrorist financing within the financial group they are part of.

The methodological guidance is subdivided into the following parts:
A.The concept and basic principles of protection of a bank against money laundering and against terrorist financing
B..Employees responsible for the implementation of tasks OF protection against money laundering and terrorist financing
C. Program of bank activities against money laundering and terrorist financing
D. Acquaintance, education of employees, information system
F. Identification, delaying and reporting of an UBO
G. Measures against terrorist financing
H. Preservation of data and documentation
I. The ensuring, system and performance of internal control

To an adequate extent and taking into account the circumstances, the text of this methodological guidance, which relates to a bank, the statutory body of the bank, a member of the statutory body of the bank or the chairman of the managing board of a bank and the employees of the bank, also applies to the branch office of a foreign bank, the head of the branch office of a foreign bank, the deputy head of the branch office of a foreign bank and to the employees of the branch office of a foreign bank.

A.THE CONCEPT AND BASIC PRINCIPLES OF PROTECTION OF A BANK AGAINST MONEY LAUNDERING AND AGAINST TERRORIST FINANCING

The basic duties and rights aimed at protection against money laundering and terrorist financing are regulated by the Act and the AOB.

In addition to the Act and the AOB, a Bank shall create its regulations and particular procedures on the basis of decrees of the National Bank of Slovakia, particularly the Decree of the NBS No. 12/2004 on risks and the risk management system as amended by Decree of the NBS No. 15/2006, as well as on the basis of its own articles of association. In doing so, the bank takes into account its business objectives, the existing clientele, the extent of banking activities and products (types of transactions) and the related potential threat of their misuse for the purposes of money laundering and terrorist financing.

The articles of association of the bank define the organizational structure of the bank and the bank management system, the responsibilities of persons and units and within those issues also the management of risks, to which the bank is exposed during its activities. The protection against money laundering and terrorist financing shall be part of the risk management in the bank.

The bank must have its own concept of protection against its misuse for money laundering and terrorist financing (hereinafter referred to as "bank protection concept") both with respect to its customers and with respect to its own employees, who, in performing their work duties, could misuse their job assignment in the bank for a purpose associated with money laundering or terrorist financing. The bank protection concept is adopted by the statutory body, with the concept having to be

a) reflected in the organizational structure of the bank and its internal regulations in the form of adequate procedures and activities and
b) continuously put through and implemented by members of the statutory body, managerial employees[1] and employees who perform the financial operations of the bank's customers at the individual operations of the bank.

Within the bank protection concept, the statutory body should declare and publish its objective and idea as to how to prevent a misuse of the bank for money laundering and terrorist financing. Such a position of the statutory body should be clearly announced not only to the employees, but also to the customers of the bank and to the public, e.g. by publishing for example at the operation premises of the bank, on the web site of the bank or in the annual report of the bank.
The bank protection concept includes the setting of basic preconditions and conditions for an ongoing implementation of measures for protection against money laundering and terrorist financing in the conduct of banking activities and implementation of transactions with customers in areas regulated by the Act and in parts B to I of this methodological guidance.

[1] Art. 7 (20) of Act No. 483/2001 Coll. on banks and on amendments to certain acts as amended

B. EMPLOYEES RESPONSIBLE FOR THE IMPLEMENTATION OF TASKS OF PROTECTION AGAINST MONEY LAUNDERING AND TERRORIST FINANCING

The overall protection of a bank against money laundering and terrorist financing is the responsibility of the statutory body of the bank. The bank shall set, by means of an organizational measure, a member of the statutory body (the chairman of the managing board or another managerial employee) as the person responsible for proper protection of the bank against money laundering and terrorist financing. The person in charge of the management of the said field is responsible, together with the designated person, for the implementation of the bank protection policy.

The practical implementation of the main tasks, the compliance with and the ongoing updating of the procedures of the bank in the field in accordance with legal regulations, articles of association of the bank and international standards are the responsibility of the designated person.
In banking terminology, or the terminology of international institutions enforcing the principles of prevention of money laundering and terrorist financing, the term "anti-money laundering compliance officer" is in general use; the term refers to an employee of the bank (or a financial or other institution) who ensures the meeting of the tasks of protection against money laundering and terrorist financing. Because the Slovak language has no adequate expression for such a position or office, the methodological guidance uses the term "designated person" or the abbreviation "DP" in accordance with Art. 20 (2) h) of the Act.

Within the bank's duty to subdivide and regulate the powers and responsibility for protection against money laundering and protection against terrorist financing in its articles of association[2], the bank shall regulate the status of the DP in such a way that it is directly subordinated to the highest management level of the bank in terms of organization. The DP is active within the headquarters of the bank. The bank shall ensure full-fledged deputisability of the DP by determining a deputy to the DP.
If the bank also establishes a unit responsible for the conduct of activities necessary to ensure the tasks of the prevention system (hereinafter referred to as the "prevention unit"), the DP is the head of the unit. The tasks of the organizational unit include the responsibility for the preparation of the necessary regulations and procedures and the fulfilment of management and control tasks in this field.

A sufficiently independent status of the DP, the deputy to the DP and of the prevention unit in the structure of managerial employees and organizational units is an important element of the system of protection against money laundering and terrorist financing. The incorporation of the DP in the organizational structure of the bank contains the following elements guaranteeing a relatively independent status of the DP, the deputy to the DP and the prevention unit:
- the appointment and discharge of the DP and the deputy to the DP and by the statutory body, following a previous discussion with the supervisory board of the bank or with its chairman,
- the prescription of the powers and duties of the DP and the deputy to the DP in their job descriptions,
- separation from units ensuring for the customers of the bank the conduct of transactions or financial operations of the customers,

[2] Art. 23 (1) h) of Act No. 483/2001 Coll. on banks and on amendments to certain acts as amended

- unlimited access of the DP and deputy to the DP to all documents and databases of the bank,
- independent decision-making of the DP and the deputy to the DP when assessing the unusualness of the business operations (hereinafter referred to as "UBO") of the bank's customers, of which it has been notified by the competent employees of the bank within the internal notification system,
- decision-making regarding the sending of a report on the UBO to the financial intelligence unit (hereinafter referred to as the "FIU"),
- the control function of the DP, the deputy to the DP and the prevention unit with respect to the units and competent employees ensuring the conduct of transactions or financial operations of the customers,
- separation of the DP, the deputy to the DP and the prevention unit from the internal control and internal audit unit in the organizational structure of the bank, while simultaneously preserving their activity for subsequent control performed by the internal control and internal audit unit.

Within the selection procedure for the office of a DP and a deputy to the DP, the bank requires the candidates to prove their integrity, adequate education and an appropriate professional experience. The DP and the deputy to the DP are obliged to exercise their offices with due diligence. They are responsible for drawing up the appropriate internal regulations, educating the competent employees, adopting internal notifications of a UBO and the evaluation thereof, making decisions on reporting UBO and timely reporting of UBO to the financial intelligence unit.

The duties and rights of the designated person comprise above all

- ensuring the implementation of the bank protection concept,
- drawing up and ongoing updating the internal rule for protection against money laundering and protection against terrorist financing, cooperation in drawing up possible associated regulations related to this issue for the individual units of the bank, types of transactions and financial operations of customers,
- cooperation with the internal control and internal audit unit in the procedure under Art. 41 (2) AOB, as well as the powers to participate in the process of commenting or evaluation of new types of transactions (products) of the bank under preparation in terms of the risk related to money laundering and terrorist financing, and to express a dissenting opinion to the introduced new types of transactions, if it represents a disproportionate exposure to that risk for the bank,
- organizing the education of the competent employees of the bank and of newly employed employees participating in the implementation of transactions and financial operations of the customers,
- accepting internal notifications of a UBO,
- reporting UBO to the financial intelligence unit and maintaining work contacts with the FIU on an ongoing basis,
- monitoring the compliance with internal regulations and procedures for this field, including the conduct of controls with respect to the assessment and notification of a UBO by the competent employees in connection with the implementation of transactions and financial operations of customers,
- regular provision of information to the statutory body of the bank (at least, however, two times a year and, if needed, also extraordinarily) on the results of its own activities and of the activities of the prevention unit, separately on the number and content of the detected

UBO, the most frequently recurring UBO types, the number and content of reports on a UBO sent to the FIU, the number and content of unsent reports and the reasons for the decision not to report,

- proposing measures to the statutory body in connection with UBO being assessed and detected UBO, as well as deficiencies in the area of bank protection.

Some of the competent employees of branch offices of the bank, or other external workplaces, can be charged with the conduct of activities related to protection against money laundering and protection against terrorist financing for the branch. The employee is in ongoing work contact with the DP. However, internal notifications of detected suspicions on UBO sent by the competent employees from branch offices of the bank to the designated person at the headquarters of the bank cannot be conditional on a consent of the specified branch employee in charge or another managing employee of the branch.

C.PROGRAM OF BANK ACTIVITIES AGAINST MONEY LAUNDERING AND TERRORIST FINANCING

The articles of association under Art. 23 of the AOB regulate the organizational structure of the bank and its internal management system. In the articles of association, the bank is obliged to subdivide and regulate the powers and responsibility in the bank for protection against money laundering and terrorist financing. The articles of association shall also regulate a risk management separated from the management of banking activities including the management system for risks, to which the bank is exposed in the conduct of its activities. The regulation of the risk management also includes protection of the bank against money laundering and terrorist financing.

The bank shall draw up a Program of Bank Activities against Legalization and Terrorist Financing (hereinafter referred to as the "Program"). The internal rule containing the Program is approved by the statutory body of the bank. The Program is based on generally binding legal regulations, particularly on the Act, the AOB, the Decree of the NBS on risk management and on methodological guidances of the FIU, as well as on the articles of association of the bank. The Program concretizes the bank protection concept. It regulates the basic principles and procedures of the bank for protection against money laundering and against terrorist financing, above all the facts under Art. 20 (2) of the Act. It also contains specific measures, duties and procedures of the DP, the prevention unit and the competent employees of the bank, in the conduct of banking activities, the types of transactions and financial operations of customers in terms of requirements required by protection against money laundering and against terrorist financing, the control rights of those entities and control rights of the internal control and internal audit unit (part I).

When creating the Program, the bank takes into account its own specific features, particularly its size and market share, organizational breakdown, the type and scope of the permitted and conducted banking activities, the types of transactions and their extent and specific features, the type and amount of customers and the specific features and extent of operations of those customers. The Program contains not only information on legal provisions, responsibilities of employees, but also particularly all operational procedures and duties of the employees under the circumstances of the bank during the conduct of the relevant types of transactions and financial operations of customers.

The Program of Bank Activities against Legalization and Terrorist Financing regulates primarily

- the determination of the group of positions or offices responsible for complex protection of the bank against misuse for money laundering and terrorist financing and for policy and implementation of procedures; the creation of the organizational system of such protection including a member of the statutory body, DP, or prevention unit and competent employees performing financial operations for customers (hereinafter referred to as "competent employees"),
- the determination of the person, as defined in Art. 20 (2) h) of the Act, who is responsible for protection against money laundering and terrorist financing, accepting notifications of an detected UBO from the organizational units of the bank, evaluation of those notifications and reporting UBO to the financial intelligence unit, and who ensures the ongoing work contact of the bank with the FIU or with a body in charge of criminal proceedings,
- the setting of basic tasks of the competent employees, their procedure in detecting UBO and notifying the DP (if needed, also the specimen form of internal notifications on UBO) and the way of ensuring protection of the competent employees in connection with the UBO detected by them and of which the designated person has been notified,
- the duty to identify customers in the conduct of transactions and individual financial operations and the duty to conduct verification of such identification,
- the duty to record the performed identification and verify the identification of customers, as well as of all financial operations performed for customers,
- the duty to preserve records on the identification and verification of the identification of customers and on financial operations performed for customers,
- an overview of the know types of UBO by activities and types of transactions performed by the bank,
- the evaluation and management of risks – procedures during the assessment of customers based on a risk-based approach and risk analyses, taking into account the results of the original and ongoing identification of customers and its verification by types of transactions and types of accounts,
- the determination of the way and extent of the conduct of diligence with respect to the customer based on the results of risk evaluation under Art. 10 (4) of the Act,
- the procedure of assessing whether the transaction in preparation or the transaction being performed is unusual; the detailed features of unusualness, by means of which an unusual business operation of a customer can be identified; this procedure should be based on a previous analysis of business operations performed by a particular customer, using electronic information systems or programs,
- the procedure of the DP in assessing a UBO, of which it has been notified by the competent employees, in reporting UBO to the financial intelligence unit, and the way and extent of implementation of what is called feedback within the bank regarding internal notifications of a UBO,
- the procedure of the competent employees and DP in delaying an unusual business operation under Art. 16 of the Act,
- the content and time schedule of training of employees, who can get in contact with the UBO; the preparation of employees for ensuring tasks of bank protection against money

laundering and against terrorist financing in the conduct of particular banking activities, types of transactions and operations of customers,

- the duty to maintain confidentiality regarding an internal notification of a UBO and its reporting to the FIU and on performed measures of the FIU (Art. 18 of the Act), above all with respect to the customer concerned, as well persons that are in a certain relationship to the customer (e.g. other persons authorized to dispose of the customer's account, or if the persons are several owners of the funds in one account or owners of a legal person or other beneficial owners enjoying the benefits related to the operation), as well as to third persons, except for exceptions specified by the Act,
- measures that will prevent a misuse of the position or office of the competent employees for wilful involvement in money laundering or terrorist financing in the exercise of their office,
- the way and set time periods for the preservation of data and documents (see part H for details),
- the way of checking compliance with duties resulting from the Act and from the Program; the determination of responsibility for the check and regular reports in connection with the detected deficiencies, containing an evaluation of compliance with obligations, the detected deficiencies and proposals of measures to eliminate the deficiencies (internal audit), including the submission of such reports to the statutory body of the bank (to the head of the branch office of a foreign bank).

The issue of protection against money laundering and protection against terrorist financing requires that the Program be drawn up as a self-contained regulation, which is available to the competent member of the statutory body, DP and all competent employees.
The bank is obliged to update the Program adequately not only in the case of a change to the relevant generally binding regulations, but also in the case of changes related to its own conduct of activities and types of transactions, as well as in the case of changes to its organizational structure.
The branch office of a foreign bank also follows internal regulations in this field[3], which have to correspond to the requirements resulting from the Act, the AOB and regulatory measures of the National Bank of Slovakia and the FIU in terms of the quality of their content.

D.ACQUAINTANCE, EDUCATION OF EMPLOYEES, INFORMATION SYSTEM

1. Acquaintance of the employees

The managers, as well as employees of a bank, have to realize that participation of bank customers in money laundering or terrorist financing can threaten the bank. Ultimately, the bank can suffer financial losses, if it performs operations with income or funds stemming from any criminal activity, and its credit is also threatened or lost. Not only banks as legal persons are subject to sanctions for failure to fulfil or violation of duties in this field, but members of the statutory body, supervisory board, managerial employees performing control and competent employees, who are in direct contact with the customers and implement the instructions of customers for the conduct of transactions and financial operations, can be also affected personally.

[3] Art. 5 (2) in conjunction with Art. 20 of the Act

The bank shall publish information for employees as to who performs the office of the DP and who is the deputy to the DP. The information shall also contain an overview of the basic elements of the prevention system, which is applied in the bank, on the basic rights and duties of the DP and the deputy to the DP, as well as on the ensuring of protection of the competent employees detecting UBO.

The effectiveness of preparation of the competent employees and their becoming duly familiar with the duties and rights are decisive for the success of the continuous process of protection against money laundering and against terrorist financing. The statutory body and the DP must ensure acquaintance of the employees with the responsibility of the bank, as well as personal responsibility of managerial employees and the competent employees of the bank in this field.

The bank shall set an optimum regime and way of

- informing its competent employees of the principles, procedures, duties and rights within protection against money laundering and terrorist financing
- making the Program and, if needed, other relevant regulations accessible to the competent employees and
- organizing training and educational events for the competent employees.

When informing and educating the employees, the bank takes into account its conditions, particularly its size and organizational subdivision into branch offices and smaller workplaces, banking activities and types of transactions and financial operations performed for customers, so that all necessary information gets to all employees, for which it is destined. It is important that the model of providing information to employees on the part of the statutory body, the DP and managerial employees of the bank, as well as of implementation of training of employees, is effective, flexible and fulfils the expected objective.

2. Information system at the bank

A systemic approach to the risk management of the bank and to ensuring protection of the bank against money laundering and terrorist financing requires the setting up of an appropriate information system at the bank and a continuous and timely flow of information between the individual management levels of the bank, including the statutory body of the bank, the DP, the deputy to the DP and the prevention unit, internal control and internal audit unit and the competent employees. In addition to continuous and timely flow of information, the systemic approach also requires the setting up and maintenance of internal information flows at the individual management levels of the bank. In a broader sense, it is the system of acquiring, processing, evaluating, passing on and using information concerning this field. Part of the system are information flows in the process of the individual activities of the bank and the performed types of transactions during protection against money laundering and terrorist financing.

It is important that the management of the bank regularly receive information on the functionality and effectiveness of the system of prevention of money laundering and terrorist financing at the bank. The information should serve for the statutory body of the bank and the management employees as source material for the adoption of principal and systemic measures for the elimination of possible system deficiencies and for the prevention of the necessary level of the

prevention system. The information should created particularly by the internal control and internal audit unit of the bank and the DP with the prevention unit.

The bank is obliged to ensure and use its own information system

- for the transfer of information, towards the competent employees, on the principles of protection against money laundering and terrorist financing, the procedures, duties and rights and the related ensuring of day-to-day tasks,
- to make the Program and other relevant internal regulations accessible to the competent employees,
- for the transfer of necessary information between the member of the statutory body of the bank responsible for protection against money laundering and terrorist financing (or the chairman of the managing board) and the DP,
- for the transfer of information between the competent employees and the DP and vice versa, including internal notification of an UOC,
- for record keeping, i.e. recording, processing and updating of data on customers and recording and monitoring of business operations of customers,
- to acquaint the statutory body or its competent member (or, if applicable, the chairman of the managing board) with the results of the control conducted by the DP and the internal control and internal audit unit, as well as to inform the competent employees on those results,
- for the transfer of information between the DP and FIU, including the reporting of UOC and provision of other necessary information and source documents to the FIU, as well as the provision of what is called feedback from the FIU to the bank.

A regular, consistent acquisition and evaluation of information in the process of identification and verification, monitoring of the business relation and assessment of transactions, internal notification of transactions with features of a UOC and reporting of UOC to the financial intelligence unit are integral parts of the duties of employees involved in this process.
The form, content and rules of his information flow should be set by the bank depending on its size, orientation and extent and on the complexity of the activities conducted by the bank and the types of transactions and services offered by the bank, as well as characteristic features of the customers and their transactions.
The information system is supposed to comply with specific conditions of the bank and, in terms of technology, it has to have such parameters that the bank is capable of fulfilling duties resulting for the bank as the obligor from the Act.

An important part of the information system of the bank os the electronic information system (hereinafter referred to as the "EIS"), which meets the requirements of the Act set for banks in terms of hardware and software, with the aim of ensuring sufficient quality of protection against money laundering and terrorist financing.

The EIS, recording and processing data on customers of the bank and their financial operations, must take into account requirements regulated in Art. 9 (e) of the Act. If the customer is a natural person, the EIS must contain record at least with the name, surname, data of birth or birth number and account numbers of the customer, and in the case of a natural person –entrepreneur also the identification number, if it has been assigned to him. If the customer is a legal person, the EIS

must contain records containing at least the name (business name) and identification number of the customer.

At the same time, the EIS must contain information/records on the nature of the business relationship of the customer. The nature of the business relationship is given by the type of transaction under Art. 9 i) of the Act or just by the transaction under Art. 9 h) of the Act. The EIS and the way of using it are supposed to enable to identify UBO performed by customers or, if applicable, also to monitor their course or development, as well links between financial operations of a certain customer and, inasmuch as possible, also between unusual business operations of various customers.

Data on politically exposed persons (Art. 6 of the Act) and on fictitious banks [Art. 9 (d) and Art. 24 (1) of the Act], which the competent employees have acquired in the conduct of their work tasks, constitute a special part of information recorded and monitored by means of the EIS. The EIS is supposed to serve to the bank also for monitoring the necessary data for the purposes of keeping the register of suspicious customers under Art. 92 (6) a) of the AOB and for information exchange with other banks under Art. 92 (6) b) of the AOB. Other situations, in which the bank can use the EIS for the provision of information, result from Art. 18 (8) of the Act.

The EIS is supposed to enable that the bank provides the FIU, without delay and upon request of the FIU, with information as to whether it has or has had a business relationship with a particular person in the previous five years, as well as the nature of such a business relationship (Art. 24 (4) of the Act).

The EIS is also supposed to be capable of providing data, on time and to a sufficient extent, to the FIU, the National Bank of Slovakia – the financial market supervision unit as the supervisory authority - and to bodies in charge of criminal proceedings in cases set by the Act. Last but not least, the EIS is supposed to meet the requirements for the purposes of control for the bank's own needs and for the needs of the FIU (Art. 30 of the Act) and for statistical purposes.

3. Employee education

The effectiveness of protection of the bank against money laundering and terrorist financing depends on the attitude of its management and employees to this issue and on the acquisition of basic legal regulations, the Program and other related internal regulations of the bank.

The heterogeneity of the performed banking activities and types of transactions and particularly the heterogeneity of the customer structure also include a varying degree of the risk of money laundering and/or terrorist financing. The competent employees must have all necessary information on banking activities and types of trades performed by the bank, which they will implement for the clients and must learn as early as possible the criteria (features of unusualness) for the assessment or detection of UBO. Those employees have to be able to assess the action of the bank's customers, as well as the content of financial operations conducted by the customers in terms of their degree of riskiness, unusualness or suspiciousness.

The competent employees are an important element in the prevention of a misuse of the bank for money laundering and/or terrorist financing. Likewise, however, the can be its weakest element,

if they do not fulfil the set duties, or if they wilfully or unwilfully participate in the implementation of a UBO of the customer.

Before an employee assumes his employment relationship at the bank for a job or office, where he will ensure the implementation of financial operations in direct contact with customers, the bank shall convince itself based on an extract from the criminal records of the future employee that the future employee has no record of a previous criminal activity in relation to property, business or other serious criminal activity. The bank can ask the future employee for information even beyond the scope of an extract from the criminal records; in such a case, however, the bank should take into account that according to the Criminal Act, if the conviction of a person has been expunged from its criminal records, the person is to be treated, as if it had not been convicted. The bank should also request sufficiently satisfying references from the future employee or an evaluation of his previous work integrity, issued by his previous employer.

Within education, too, the bank shall ensure that the employees be acquainted with the consequences of a neglect or negligent fulfilment of their work duties and of a possible wilful or unwilful participation in money laundering or terrorist financing, as well as violation of the prohibition to provide information, to which the pledge of confidentiality applies, to a customer (Art. 18 of the Act).

The education of employees is supposed to contribute considerably to a situation where the competent employees acquire the prerequisites for copying with the procedures for the application of the "Know Your Customer" principle (hereinafter referred to as "KYC") and for the identification of the degree of riskiness of action of the bank's customers even after taking into accounting the classification of the customers in one of three groups for the conduct of due diligence, i.e. basic, simplified and enhanced diligence.

The bank must have a project or plan of employee education taking into account the job assignment of employees and the resulting responsibilities and duties. The plan of education or its basic principles should be a part of the Program and should set the basic outline, periodicity and content of employee training, particularly the provisions of corresponding laws, internal regulations and rules of the bank or, if applicable, of the group, to which the bank belongs, as well as an analysis of the content and circumstances of the most frequently occurring types of internal notifications of UBO within the bank or, if applicable, within the group.

The bank is obliged under Art. 20 (3) of the Act to ensure training for employees aimed at acquainting themselves with the Program at least once a calendar year and at the same time always prior to assignment of the employee to a work, during which he will fulfil tasks set by the act and the Program. Each competent employee fulfilling tasks under this act must be acquainted with the valid Program regulating the procedures for the assessment of customers and of financial operations performed by them and must have the Program always at his disposal.

Education includes training of newly employed employees and ongoing specialised professional education of the competent employees implementing financial operations of customers. The frequency of educational events is supposed to be adequate so as to enable the provision of information on new generally binding legal regulations, on the Program and on current internal regulations and to make accessible knowledge resulting from the bank's activities, from the

activities of other banking entities, as well as available knowledge based on activities of the FIU or of a supervisory authority.
Specialised education, which the competent employees are supposed to complete before they process instructions of the customers to perform financial operations, should provide them with the necessary knowledge for detecting and verifying the identity of customers when the business relationship arises and during the conduct of transactions and operations. By participating in educational events (seminars, educational stays), the competent employees acquire the prerequisites for getting to know the type of expected business activities of customers, with which their financial operations are associated, and thereby also the necessary knowledge and capability to identify facts going beyond the expected behaviour of customers and particular manifestations of their unusual business operations.

The bank is supposed to repeat the education and to add new knowledge to it, if needed, even more frequently than at a 12-month cycle, to ensure that the competent employees will be able to perform their duties and rights on an ongoing basis.

The bank shall ensure the drawing up of records on performed employee training, which shall contain the date of participation of the competent employees in the education, the content of the education, as well as the signatures of employees having completed the training. In addition, it is necessary to obtain a written confirmation from the competent employees attesting that they acquainted themselves with the Program and with related regulations regulating the procedures for protection of the bank against money laundering and terrorist financing.

E. IDENTIFICATION AND ACCEPTANCE OF THE CUSTOMER, RISK PROFILE OF THE CUSTOMER; BASIC, SIMPLIFIED, ENHANCED DILIGENCE, FUILFILMENT BY THIRD PARTIES

Basic duties of the bank in these areas are set by the corresponding provisions of the Act, particularly Art. 7, 8 and 10 to 13, as well as the AOB, particularly Art. 89 and Art. 93a.

In practice this means that the bank will implement all elements of basic customer diligence (both natural and legal person) under Art. 10 (1) of the Act always in situations stated in Art 10 (2). In the case of one-time transactions outside the business relationship, the bank identifies and verifies the identification whenever the transaction reaches a value of at least EUR 2,000.
What follows is the duty to find out whether the customer is acting on his own behalf. For the purposes of this methodological guidance, it is necessary to understand the "performance of a transaction on one's own expense" or "with one's own funds" as action on one's own behalf. Pursuant to Art. 10 (10) of the Act, it is necessary to find out this fact always in situations stated in Art. 10 (2) and in accordance with Art. 89 (3) of the AOB, even if the transaction is a transaction of at least EUR 15,000 (i.e. not only a "casual" transaction, as the Act implies).

The detection and, to an adequate extent, also the verification of the beneficial owner follows primarily the provisions of Art. 9 and 10 of the Act, with the AOB also partially dealing with this important element of the basic and enhanced customer diligence in Art. 93a. This area is one of the basic preventive measures enabling the FIU and later also bodies in charge of criminal proceedings to monitor the movements of funds and to detect also possible interconnections of natural persons and legal persons not only in the territory of the Slovak Republic, but also abroad,

by means of information exchange between the financial intelligence units of various countries. (Ideally, after the valid award of a court judgment or even during the judicial trial and in the case of a "freeze" of funds based on international sanctions, the implementation of the identification and verification of the identification of customers and beneficial owners enables to temporarily or permanently touch the funds from the application of temporary measures, such as seizure of property, up to forfeiture of property).
At the same time, this is the most work intensive and cost intensive part of the conduct of basic and enhanced diligence, in which it is extraordinarily important to apply a risk-based approach of the bank towards its customers and their financial operations. This means that it is always necessary to detect the beneficial owner; in the case of legal persons, the legal form of the company (e.g. a joint-stock company with bearer shares or a pooling of property) must not hinder the detection of the beneficial owner. The verification of the acquired information on the beneficial owner in accordance with the Act is supposed to be carried out to an adequate extent; e.g. by requesting a written declaration on the beneficial owner and subsequent verification of such information from available sources.

The importance of Art. 10 (1) a) to c) and Art. 10 (10) of the Act is highlighted in Art. 15 and 24 (2) of the Act, in which the duty to reject a new customer, to terminate the existing business relationship with the customer or to reject to perform a particular business operation, if it is not possible to conduct basic diligence, is imposed on the bank. A comparable duty results from Art. 89 (1) of the AOB. Pursuant to Art. 17 (1), the bank is obliged to report such cases immediately to the FIU.

In addition to the conduct of basic diligence, the acceptance of a the customer should include his assignment to a certain risk group in the case of a new customer; a precondition should be consistent application of the "KYC" principle, which actually means ensuring the acquisition of sufficient information on the nature of the expected transactions of the customer and any predictable design of the operations performed by him. On the basis of this, it is possible to set up a risk profile of the customer. When applying basic diligence, the bank must not enter into the business relationship with the customer, until it reliably detects all relevant circumstances related to the customer (including the detection of the beneficial owner and adequate measures for the verification of the information), as well as the nature of trading or doing business or of his other activities.
The managerial employees and competent employees of the bank must know the clients of the bank and their usual trade activities, business activities or other activities. Based on the acquired information, during the existence of the business relationship of the bank with the customer, the competent employees of the bank and their direct superior are able to assess any instruction of the customer for the disposal of funds kept in his account, in comparison with the expected behaviour of the customer. In doing this, they take into account circumstances, which can indicate a change in the nature of the business activities of the customer or a change in his usual activities and they verify such facts adequately.

The bank updates information on the customer according to the risk group, to which the customer has been classified; with this aim it requests the customer to update the data the customer provided originally or has updated earlier already, in reasonable time intervals and depending on changes related the person of the customer or his business or other activities, with which his financial operations performed by the bank are connected. The bank can perform the update also

by requesting that the corresponding form be filled in, for example once a year, unless more frequent updating is indispensable, or by agreeing with the customer upon a contract condition on the duty to report the respective changes to the bank in advance.

Pursuant to the temporary provision Art. 36 (1) of the Act, the bank shall conduct procedures to detect all possible elements of basic diligence, including the identification and verification of the beneficial owner under Art. 10 of the Act and enhanced diligence under Art. 12 of the Act, also with respect to existing customers, depending on the risk of legalization or terrorist financing, as from 31 December 2009.
In practice, this means that it is necessary to subdivide the current clientele of the bank by the risk of money laundering and/or terrorist financing, with the Act saying in Art. 10 (4) that under such a subdivision, information on the customer, type of transaction, business relationship etc. can be used. Pursuant to Art. 10 (11) of the Act, basic diligence also includes the detection whether the customer is a politically exposed person; if the person is a politically exposed person, the bank shall implement enhanced diligence.

In this connection, it is necessary to use the hitherto knowledge on customers and on the application of the prevention system at the bank from the previous version of legislation, the basis of which was UBO reporting. The Act has kept the same scope of the definition of a UBO; however, a paragraph 2 was added in Art. 4, which lists examples of transactions, which have to be considered UBO and which should be reported to the FIU (depending on the particular circumstances of the case). In addition, it is also suitable to use materials drawn up by the experts of the Financial Action Task Force (published on the internet), for example:

- the regularly published conclusions of the ongoing monitoring of countries that have considerable deficiencies in the enforcement of measures against money laundering and terrorist financing (the "FATF statement"),
- detailed evaluation reports on individual countries and their system of prevention and repression in the field of money laundering and terrorist financing (in the "Mutual Evaluation Report" form),
- the explanatory presentation "Guidance on the risk-based approach to combating money laundering and terrorist financing" of June 2007,
- the so-called list of equivalent Third Countries, which has been created based on an agreement of the EU member states in a European Commission committee (the CPMLTF – Committee on Prevention of Money Laundering and Terrorist Financing) and has been published on the web site of the FIU.

In connection with the subdivision of the customers by their riskiness, it is necessary that the bank takes into account Art. 10 (1) d) and 10 (8) of the Act, which create the duty to update the risk profile of a customer on an ongoing basis. The suitable periodicity of the updates depends on an internal decision of the bank, at any rate it is necessary to include in the internal regulation regulating the Program of the bank under Art. 20 of the Act.

By subdividing the customers by their risk profile, the bank then can apply Art. 10 (1) d) of the Act in practice – an ongoing monitoring of the business relationship leading to the identification and reporting of a UBO.

A higher riskiness of a customer requires a more detailed assessment of the customer, his action and his orders for the implementation of financial operations. Subsequently, it is necessary to adopt measures for the elimination of risks to an acceptable level.
The bank applies enhanced diligence towards a customer in situations that due to their nature can represent enhanced risk of money laundering or terrorist financing. The bank pays special attention to selected groups of entities – in addition to the above mentioned politically exposed persons (Art. 6, Art. 10 and Art. 12 of the Act), above all to poolings of property (Art. 25 (2)) and fictitious banks (Art. 24 (1)).
The bank proceeds in the same way, if the creation of

- a new business relationship or account without the physical presence of the customer and
- new correspondence relationships with foreign banks or credit institutions

is being prepared.

In line with the implemented EU directives, the Act defines only basic situations, which represent enhanced risks of money laundering and terrorist financing. However, a more stringent procedure for the identification and verification of the acquired facts and for the subsequent monitoring of the business relationships with the customer has to be applied by the bank also in other situations, according to the risk profile of the customer or according to the degree of risk of the service provided or the type of transaction for the customer (legal persons not registered in the Commercial Register, for example political parties, legal persons in the form of joint-stock companies with bearer shares, joint accounts, accounts with custodianship, etc.).

The putting through and compliance with all the above mentioned procedures and rules (identification, verification, KYC) also provides protection against frauds. At the same time, it enables the bank to select and offer from the wide range of types of transactions the types of transactions that comply with the wished of particular customers by the content and extent of their activities. It thereby helps the bank to keep customers that are not linked to money laundering and frauds and at the same time to eliminate the risk of financial losses and the risk of the loss of the bank's credit.

In Art. 13 the Act enables an already conducted basic diligence – with the exception of one part of basic diligence, which is the ongoing monitoring of the business relationship pursuant to Art. 10 (1) d) of the Act - to be used by another credit and financial institution in the application of diligence procedures with respect to the customer by means of the so-called "performance by third parties". The point is that when the preconditions specified in this provision are fulfilled, it is possible to rely an already performed identification and verification of a customer and beneficial owner and to take over the data on the identification and verification from a credit or financial institution (to the extent defined in Art. 5 (1) b) 1 to 10 of the Act), which is active in the territory of the EU (the so-called third party), including those being active in the territory of the SR. (Exchange offices and places of foreign exchange are not in the group of obligors, from which it is possible to take over the identification and verification of the customer and beneficial owner). However, the responsibility for the fact that data acquired in this way meet the requirements for the conduct of diligence towards a customer under the provisions of the Act remains with the bank having decided to rely on the "performance by third parties" procedure.
Pursuant to Art. 13 (4), the Act considers "outsourcing" to be an activity performed for the bank based on the bank's rules and regulations, therefore such situations are not considered to be a performance by third parties.

In its Art. 11, the Act defines the extent and conditions for the use of simplified customer diligence. These are situations and customer, where it is possible to acquire and verify basic information from publicly available and reliable sources – as stated in Art. 11 (1) of the Act. Art 11 (2) regulates the types of products, for which it is possible to use simplified customer diligence. The fact is important that before the bank decides to use simplified diligence, it is necessary to acquire information on the customer or type of transaction (product), which justify the application of simplified diligence. The use of simplified diligence represents by no means an exception from the duty of ongoing monitoring of the business relationship [Art. 10 (1) d) of the Act] or from other duties defined by the Act, so that it is possible to comply with Art. 14 and 17 of the Act, as well as other provisions, including the duties to process and preserve data pursuant to Art. 19 and 20 of the Act.

In connection with the use of simplified diligence, the possibility of using the list of the so-called Third Countries, which has arisen by an agreement of the EU member states and is deemed to be a minimum list. The list has been published on the web site of the FIU. However, the fact that a country is not listed in the list does not preclude the allocation of a particular customer from the country to a higher risk. Indeed, it is always necessary to apply the duties pursuant to Art. 10 (1) d) and Art. 10 (4) and Art. 10 (8) of the Act consistently.

F. IDENTIFICATION, DELAYING AND REPORTING OF AN UBO

To identify unusual business operations by the bank, it is decisive to apply Art. 2 to 4, Art. 10 to 12, Art. 14 and Art. 20 of the Act.

Pursuant to Art. 14 (1) of the Act, the bank is obliged to assess whether the transaction under preparation or transaction being performed is unusual and according to Art. 14 (2) a) of the Act it is obliged to pay special attention to all complicated, unusually large transactions and all transactions of unusual nature, which have no economic purpose or obvious legal purpose. At the same time, the bank is obliged to examine to the largest extent possible the purpose to those transactions, and it has to conduct a written record on those transactions for control purposes.

Pursuant to Art. 4 of the Act, a UBO is a legal act or another act suggesting that by performing the act money laundering or terrorist financing can occur. Art. 4 (2) of the Act sets out a demonstrative list of UBO. However, in each UBO stated in this provision, there are several features of unusualness (e.g. an unusually high volume of funds without an obvious economic or legal purpose etc.), which the bank has to assess, while at the same time applying the KYC principle. Only on the basis of such a procedure, it is possible to assess in a qualified way, whether the customer's business operation being prepared or performed is or is not unusual. In its Art. 4, the Act does not regulate any criteria, e.g. in the form of limit sums of funds, that would lead to an automatic establishing that a certain type of financial operation is automatically a UBO. The decisive element for the assessment of business operations of the customer is the application of the KYC principle and qualified identification of so-called features of unusualness, which are stated in the individual provisions of Art. 4 (2) of the Act, as well as other features and criteria, which the bank has to set for itself depending on the subject-matter and extent of its activity and type and extent of the performed transactions and financial operations for customers, within the creation of an overview of the forms of UBO [Art. 20 (2) a) of the Act].

The conditions for a qualified application of the UBO principle result from the duties of the bank and customer set in the Art. 10 to 12 of the Act. The crucial provisions are Art. 10 (1), (4) and (5) and, if applicable, also Art. 11 (3).
The procedure under Art. 10 (1), and, if applicable, 11 (3) of the Act will enable a bank to convince itself to an adequate extent of the true identity of each customer and to identify the purpose and planned nature of business activities, which the customer is likely to conduct. At the same time, this procedure is the starting point of the bank for the creation of a risk profile of the customer, subsequent determination of the extent of diligence pursuant to Art. 10 (4) of the Act and for accepting the customer. Then, depending on the result, the bank applies the procedures within basic diligence under Art. 10 of the Act or simplified diligence under Art. 11 of the Act or enhanced diligence of Art. 12 of the Act.
Irrespective of whether the bank proceeds under Art. 10, Art. 11 or Art. 12 of the Act, it is, among other things, obliged to proceed according to Art. 14 of the Act each time. Thus, the bank has to assess in each case, whether the transaction being prepared or performed is unusual (Art. 14 (1) of the Act) and pay special attention to all complex, unusually large transactions and all transactions of unusual nature, which have no obvious economic purpose or obvious legal purpose and make a corresponding record on them under Art. 14 (3) of the Act.

The bank performs qualified assessment of transactions being prepared or performed under Art. 14 of the Act at various levels. The assessment process is done in "the first line", where the employees of the bank are in contact with the existing or potential customer, furthermore within ongoing monitoring of the existing business relationship and within the subsequent/retrospective assessment of the customer's transactions.

1. "First-line" assessment of trades
The assessment of a customer's transactions is performed "in the first line" by the employees of the bank, which are in contact with the customer when fulfilling their duties, particularly those processing the customer's orders for the execution of his transactions or financial operations. These are primarily cashiers, employees ensuring the implementation of money transfers or payment transactions and other employees involved in the provision of services to customers and in data processing, as well as employees directly superior to those employees. The firs-line assessment of transactions depends on the expertise and preparedness of the competent employees, which they have acquired with obligatory training (Art. 20 (3) of the Act).
The bank's Program against legalization and terrorist financing must be available continuously to each competent employee, whether in paper or electronic form, and the employee has to learn it and proceed according to it. At this stage, the employee of the bank has to adhere particularly to Art. 10 (1) or, if applicable, to Art. 11 (3) of the Act, which enables him to convince himself adequately on the actual identity of the customer and to get to know the purpose and planned nature of business activities that the customer is likely to conduct. This procedure is also the starting point for the customer being accepted by the bank, for the creation of the customer's risk profile and for determining the extent of diligence towards the customer under Art. 10 (4) of the Act.

Here, too, the crucial element for the assessment of the business operations of the customer is the appropriate application of the KYC principle and its procedures and qualified identification of features of unusualness. The procedure will enable a competent employees to assess the

customer's transactions being prepared or performed in accordance with the overview of UBO forms [Art. 20 (2) a) of the Act] and reveal those transactions, which are unusual with respect to the client and his otherwise usual transactions. If the competent employee assesses the transaction being prepared or performed as unusual, he will make a written record on that transaction under Art. 14 (3) of the Act and will notify the designated person of this finding without delay (hereinafter referred to "notification of a UBO").

2. Assessment of transactions within ongoing monitoring of the business relationship

Depending on whether a business relationship is being entered into [Art. 10 (2) a) of the Act] or the transaction is casual [Art. 10 (2) b) or, if applicable, c) of the Act], the competent employees of the bank assess the customer's transactions also within ongoing monitoring of the business relationship. The assessment of transactions being prepared or performed within the ongoing monitoring of the business relationship is specific in that the business relationship has already arisen and goes on [Art. 10 (2) a) of the Act]. Where applicable, the customer is known to the bank, because he has conducted several casual transactions already [Art. 10 (2) b) or c) of the Act]. Thus, this is not the first contact with the customer and the bank can take into account the existing risk profile of the customer and the history of transactions conducted by him.

The procedure under Art. 10 (1) d) of the Act, including the verification of the completeness and validity of identification data and information pursuant to Art. 10 (8) of the Act and the customer's duty under Art. 10 (5) of the Act, form the basis for the ongoing monitoring of the business relationship. This type of monitoring requires that risk profiles of customers be creates and they be sorted by the possible risk of money laundering or terrorist financing under Art. 10 (4) of the Act. Ongoing monitoring of the business relationship requires the use of an appropriate electronic information system, which will enable the bank, in line with risk-oriented prevention, to create financial or other criteria or limits being among the features of unusualness of business operations of customers, which would separate certain monitoring process levels, corresponding to the degree of riskiness of the operations performed by the customers. The set criteria or limits, defined by the bank for that purpose, must be regularly verified, so that it is possible to determine their adequacy with respect to the detected risk levels.
The bank also has to re-evaluate the adequacy of the existing system and individual processes of protection and prevention.

For assessing transactions, those transactions of the customer being prepared or performed will be important within ongoing monitoring of the business relationship, which do not correspond to a known or expected activity of the customer. Such transactions of the customer must be subject to evaluation (Art. 14 (1) of the Act) and a written record must be made on them (Art. 14 (3) of the Act). Based on the results of further assessment of the individual circumstances of the transaction and taking into account the overview of UBO forms [Art. 20 (2) a)], the DP can conclude that there is no UBO in the given case. If this is not possible only based on information on the customer available to the bank already, it can, according to circumstances, require further necessary information and documents according to Art (5) of the Act from the customer.

In cases where the DP is unable to justify the customer's transactions, which do not correspond to the known or expected activity of the customer, not even using such procedure, it shall be sufficient that those operations only suggest that performing them can lead to money laundering

or terrorist financing and the DP is obliged to proceed under Art. 17 of the Act, i.e. to report the UBO to the financial intelligence unit.

The assessment of transactions within the ongoing monitoring of the business relationship is performed depending on the transaction by the competent employees, as well as the DP.

3. Assessment of transactions within the subsequent/retrospective assessment of the customer's transactions

A means of subsequent monitoring of the transactions of the customer is for example random selection of performed transactions within the performance of control on the part of a managerial employee, superior to the competent employee, who has implemented instructions and operations of the customer, as well within the performance of control carried out by the DP and the internal control unit (part I).

4. Internal notifications of a UBO

All internal notifications of a UBO sent by the competent employees to the designated person must be documented according to Art. 14 (3) of the Act and must be available for control purposes under Art. 29 of the Act. The DP keeps files of and preserves the notifications of internal notifications of an UBO including the function, name, surname, designation of the branch office or bank unit and all data on the customer and transaction in question.

The DP, as well as the competent employees of the bank, including the managerial employees (and members of the statutory body), which participate in the assessment of transactions according to Art. 14 of the Act, are obliged to maintain confidentiality on a reported UBO and on measures performed by the FIU (Art. 18 of the Act), including the fulfilment of duties according to Art. 17 (5) and Art. 21 of the Act. Thus, the bank must have set a procedure from the detection of a UBO up to the reporting of a UBO performed without delay, including the procedure and responsibility of the employees assessing the transaction.
However, the bank cannot invoke the pledge of confidentiality towards the National Bank of Slovakia and the Ministry of Finance of the Slovak Republic in connection with performance of supervision and control pursuant to Art. 29 of the Act (Art. 18 (5) of the Act). Provided that the provided information is used only for the purposes of preventing money laundering or terrorist financing, the pledge of confidentiality does not apply to the provision of information between credit or financial institutions under the conditions stated in Art. 18 (8) a) and c) of the Act.

According to Art. 92 (6) a) of the AOB, the bank can keep a register of customers, which have committed acts assessed as a UBO, and to which international sanctions apply, and under Art. 92 (6) b) the AOB it can provide other banks with information from that register even without the consent of the customer (provided that the data provided is protected).

Following the acceptance of the internal notification of an UBO, the DP can confirm the acceptance of the notification of an UBO to the competent employee, who has sent the notification. The confirmation should contain a notice regarding the pledge of confidentiality under Art. 18 of the Act. Where the bank has an electronic system for internal report collection, which enables the competent employee to monitor the status or acceptance of a lodged internal report on a UBO by the designated person or prevention unit, an individual confirmation of the acceptance of such a notification is not necessary.

The internal notification of a UBO, or the action of the customer and the transaction or financial operation, to which the notification applies, must be subject to evaluation (assessment) by the designated person, which can decide, whether this is a case of a UBO or not, based on the results of further assessment of the individual circumstances of the transaction and taking into account the overview of UBO forms [Art. 20 (2) a) of the Act]. If a decision is not possible only based on information on the customer being already available to the bank, it can, according to circumstances, require further necessary information and documents pursuant to Art. 10 (5) of the Act from the customer. If the designated person reaches the justified conclusion that the UBO it has been notified of is no UBO, it has to provide written documents of that decision and has to continue preserving all related data, written source documents and electronic documentation.
In cases where the DP cannot reach a conclusion that the transaction is no UBO not even using such procedure, it is sufficient, if the transaction or financial operation, of which it has been notified, suggests that performing them can lead to money laundering or terrorist financing and the DP is obliged to proceed pursuant to Art. 17 of the Act, i.e. to report the UBO to the financial intelligence unit.

According to Art. 17 (1) of the Act, a UBO or an attempt to perform it must be reported to the FIU without undue delay, i.e. at the next opportunity. Each time, the particular circumstances of the situation, in which the detection and reporting of the UBO is implemented, have to be taken into account and the UBO has to be reported as early as possible. The decision of the DP to report the UBO must not be conditional on the consent or approval by any other person.
The report on a UBO has to contain data set by Art. 17 (3) and (4) of the Act. The designation of the report on each UBO should take the form: serial number/year/character code of the bank, e.g. 1/2009/SUBA.
UBO reporting can be done in writing, in electronic form or by phone (in such a case the UBO has to be also reported within 3 days in person, in writing or by electronic mail). The specimen of the form of the report on an UBO is issued by the FUI.
Additions to the report on an UBO on the bank's own initiative can be performed not later than within 30 days. After that time limit, it is necessary to report additionally acquired information and source documents as an additional UBO. In the additional UBO, the bank shall state, with which UBO the additionally acquired information is associated.

5. UBO delaying
Pursuant to Art. 16 of the Act, the bank shall delay an UBO, i.e. a certain transaction (Art. 9 h)) that would be otherwise performed. Unless the transaction is not completed or performed, e.g. if the customer does not lodge a corresponding charging order, the bank has no transaction to delay.

Pursuant to Art. 16 (1) of the Act, the bank is obliged to delay a UBO until it is reported to the FIU, always taking into account the operational and technical possibilities, as well as the time when the business operation was or should heave been assesses as unusual. For example, a transaction of a customer assessed within the subsequent/retrospective assessment of transactions of the customer cannot be delayed anymore.

The bank is obliged to delay a UBO, if there is an imminent danger that performing the UBO can obstruct or make substantially more difficult the seizure of income from criminal activity or funds destined for terrorist financing, or if it is requested to do so in writing by the FIU (Art. 16

(2) of the Act). The time limit starts to run from the time when a certain UBO had to be performed and lasts for no more than 48 hours. This time limit can be prolonged, by a maximum of 24 hours, based on a notification of the FIU that the FIU has committed the case to bodies in charge of criminal proceedings. Consequently, the total period of delay of the UBO can lasts for 72 hours.

G. MEASURES AGAINST TERRORIST FINANCING

1. Definitions of terrorism and terrorist financing

Terrorism represents one of the most serious ways of violating values, such as human dignity, freedom, equality and solidarity and observance of human rights and fundamental freedoms, on which the European Union is founded. It also represents one fot he most serious attacks on the principle of democracy and the principle of rule of law, which are common to the member states and on which the European Union is founded.
Pursuant to Directive No. 2005/60/EC, terrorist financing means the provision the provision or collection of funds, by any means, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Decision 2002/475/JHA of 13 June 2002 on combating terrorism.

2. Duty to report

Within protection against terrorist financing banks use analogous procedures with respect to customers as in the case of protection against money laundering, including reporting UBO, related to terrorist financing, to the FIU.

The bank is obliged under Art. 91 (8) of the AOB to provide the Ministry of Finance of the Slovak Republic within the time limits set by the ministry (time limit of one quarter) a list of customers, to which international sanctions introduced under Act No. 460/2002 Coll. on the performance of international sanctions ensuring peace and security as amended (hereinafter referred to as "Act No. 460/2002"). The list provided also has to contain the account numbers and the balance on the accounts of those customers, i.e. the so-called sanctioned persons.

The bank is obliged to report an UBO to the financial intelligence unit without undue delay (Art. 17 () of the Act). The Act defines an UBO, among other things, as a transaction, for which it is justified to assume that the customer or beneficial owner is a person, against which international sanctions are being performed, or a transaction, for which it is justified to assume that its subject-matter is, or is to be, a thing or service, which can be associated with the thing or service, with respect to which the sanctions under Act No. 460/2002 are performed.

3. Consolidated list of terrorists

Lists of sanctioned persons (natural persons and legal persons) are part of annexes to individual regulations and decisions of the European Communities (hereinafter "EC"), which oblige all financial institutions of the member states to immediately freeze the financial and economic sources of sanctioned persons from states set in the annexes to the individual regulations and decisions of the EC. The EC regulations and decisions in question, regarding only sanctioned

entities and complex restrictive measures, including a consolidates list, which contains names and identification data on all persons, groups or entities, to which the financial restrictions of Common Foreign and Security Policy apply, are published on the web site.

4. Sanctions

Act No. 460/2002 defines international sanctions as the whole of restrictions, orders or bans introduced for the purpose of preserving or restoring international peace and security, which result from particular international binding documents and measures. At the same time, it defines in concrete terms international sanctions for trade and non-financial services, financial services, transportation, technical infrastructure, science and technology contacts, cultural contacts and sport contacts.

The aim of the sanctions is to keep and restore international peace and security according to the principles of the UN Charter and Common Foreign and Security Policy. This is primarily a change in the policy of a government, country, individual or group not respecting the basic principles of rule of law, violating human rights, international law or endangering security.

Restrictive measures are adopted either by transposition of sanction resolutions of the United Nations Security Council (hereinafter referred to as the "UNSC") or they are autonomous sanctions adopted by the European Union only. The sanctions are adopted by common positions of the EU and implemented at the level of the EC. In the case of autonomous sanctions, the EU can adopt even harder and broader sanctions as compared to the sanction resolution.
The current autonomous restrictive sanctions of the EU are against the countries: Belarus, Uzbekistan, Moldova.
Other current restrictive sanctions of the EU: Bosnia and Herzegovina, Montenegro, Haiti, Iraq, Iran, the Democratic People's Republic of Korea, Lebanon, Liberia, Macedonia, Myanmar/Burma, Moldova, Côte d'Ivoire, Sierra Leone, Somalia, Serbia, Syria, Zimbabwe, USA, Yugoslavia, Belarus, the Democratic Republic of the Congo, North Korea and Sudan.
Other restrictive measures: support of the implementation of the ICTY (International Criminal Tribunal for the Former Yugoslavia) mandate, Libya, the USA, other terrorist organizations (Osama bin Laden, Al-Qaeda).
The restrictive measures are adopted in several forms: for example as diplomatic sanctions, interruption of cooperation with a third country, boycott of sport or cultural events, trade sanctions, weapon embargos, financial sanctions, no-fly zones, restrictions for entry into the territory of a member state. UN sanction measures related to a weapon embargo or entry restrictions (VISA-ban) are implemented directly by a member state.

Sanction measures related to economic relationships with third countries, e.g. the freezing of financial assets and economic resources, are implemented by an EC regulation (approved by the Council) and are directly binding and applicable in the EC. The regulations are universally valid by virtue of Article 249 of the Treaty establishing the European Community and are directly applicable in all member states. As legally binding acts of the community they take presence over the laws of the Slovak Republic and financial institutions in the Slovak Republic are obliged to apply sanctions promulgated by EU regulations directly. They are also subject to legal assessment by European courts.

5. Sanction resolutions of the UN Security Council

The UN Security Council resolution against terrorism is a document, which provides the base for the criminalization of inciting to terrorist acts and recruitment of persons for such acts. The resolutions call upon countries to adopt necessary and adequate measures and to prohibit by law, in line with their obligations resulting from international law, the incitement to the commitment of terrorist acts and prevent such activity.
Due to the above mentioned facts, the sanctions are adopted by transposing the UN sanction resolution, meaning that after a UNSC resolution has been issued, it is necessary to implement the resolution as quickly as possible in an EU regulation or in a common EU position.

The most important UNSC resolutions for combating terrorism are the following resolutions: 1390/2002, 1333/2000, 1373/2001, 1378/2001, 1267/1999, 1363/2001, 1368/2001, 1269/1999, 1383/2001, 1386/2001 and they concern measures against Osama bin Laden, the Al-Qaeda, Taliban, Afghanistan, a weapon embargo, the ban on certain services, the freeze of financial assets and economic resources, the obligation of a member states for police and judicial cooperation. An overview of complex resolutions, sanction committees and UN policy against terrorism has been published on the UNSC web site http://www.un.org/Docs/sc/.

6. Procedure in the case of persons, against which sanctions have been declared according to a regulation of the Government of the Slovak Republic

In its Common Position 2001/931/CFSP as amended by Common Position 2008/586/CFSP, the European Union has published a list of sanctioned persons (natural persons and legal persons), which are brought into connection with terrorism and against which it is necessary to apply sanctions within the combat of terrorism. Persons in the list of EU Common Position 2001/931/CFSP are subdivided into "external terrorists" and "internal terrorists" (in this case these are persons marked with an "*", which are EU citizens or have their seat in the EU, for example members of the Basque organisation E.T.A. and extremist groups primarily from Spain and North Ireland).
Financial sanctions under Art. 3 of EU Common Position 2001/931/CFSP are applied against the group of the so-called external terrorists. The implementation of these sanctions is regulated by the EU Council Decision 2005/428/CFSP and by Council Regulation No. 2580/2001, which means in practice that based on directly applicable EU legislation, sanctions are binding for everybody in all EU member states and directly enforceable.
Financial sanctions are not applied against internal terrorists, because the Treaty on the EU does not enable this, in that it gives the mandate for the implementation of restrictive measures within the common market and financial services only against third countries (Art. 60 and 301 of the Treaty on the EU, i.e. the introduction of financial sanctions from the community level against the citizens of the EU has no mandate). At the EU level, only the so-called reinforced judicial and police cooperation based on Art. 4 of EU Common Position 2001/931/CFSP against internal terrorists and at the same time in accordance with Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences is applied.
However, persons stated in the list of EU Common Position 2008/586/CFSP, marked with an "*" are terrorists and based on UNSC Resolution 1373/2001 on the suppression of terrorist financing, as well as based on Art. 2 of EU Common Position 2001/930/CFSP all countries have the duty to freeze economic and financial assets to all persons, which could be designated as terrorists or provide assistance to or in any way linked to terrorist structures.

Due to the above facts, the Slovak Republic has not been able to declare sanctions against internal terrorists of the EU, therefore the freeze of terrorist activities against the said persons had to be laid down at the national legislation level. This has been done by Regulation of the Government of the Slovak Republic No. 397/2005 Coll., by which international sanctions ensuring international peace and security are declared, amended by Regulations of the Government No. 209/2006 Coll., No. 484/2006 Coll., No. 488/2007 Coll. and No. 239/2008 Coll. (hereinafter referred to as "Regulation No. 397/2005 Coll."). Regulation No. 397/2005 Coll. contains a list of those sanctioned persons, whose activity is bound to the territory of EU member states or which are EU citizens.
Banks are obliged to freeze without delay all financial and economic assets for the sanctioned persons included in the list published in the annex of Regulation of the Government of the Slovak Republic No. 397/2005 Coll.

H. PRESERVATION OF DATA AND DOCUMENTATION

For the purposes of conducting customer diligence (Art. 10 to 12 of the Act), the bank is entitled detect, acquire, record, preserve, use and otherwise process the personal data of the customer and other data to the extent stated in Art. 10 (1) and Art. 12 of the Act. The bank 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 numbers and other data and documents without the consent of the customer and to the extent stated in the said provisions of the Act.

The bank shall preserve (archive) data on the identification of customers and on the verification of identification, records on transactions and financial operations of customers and records on the establishment of the identification of beneficial owners, including photocopies of relevant documents. Pursuant to Art. 19 (1) and (2) of the Act, the bank is obliged to preserve

- data and written documents obtained using the procedure under Art. 10 to 12 of the Act for 5 years from the termination of the contractual relationship with the customer,
- all data and written documents on the customer for 5 years from the performance of the transaction.

The bank is obliged to preserve the above data and written documents even for a longer period of time than 5 years, if the FIU requests it from the bank by a written request containing the time limit and extent of preservation of data and written documents.
The above duties also apply to a bank, going to terminate its activity, until the expiration of period of time, during which the bank is oblige to preserve those data and written documents.

The procedure of the bank within the preservation of data and documentation – records related to protection against money laundering and terrorist financing is regulated by the Program of the bank, which, according to the Act, has to set in more details

- which records have to be archived (at least the data on the identification of the customer and records on his business operations and data on the identification of the beneficial owner),
- the form of records (paper form, electronic form),
- where, how and how long records are to be preserved, taking into account
    1. the termination of the contractual relationship with the customer,
    2. the performance of the transaction with the customer and

3. the written request of the FIU and the designated person (Art. 19 (3) of the Act).

The records drawn up and preserved by the bank have to fulfil the legal requirements for keeping records on customers and at the same time they have to enable

- the evaluation of the effectiveness of basic principles, as well as procedures of the bank for protection against money laundering and terrorist financing by an independent person,
- to reconstruct the course of financial operations performed by the bank for the customer,
- to identify properly and localize any customer,
- to identify all internal notifications of an UBO and external reports on an UBO,
- to fulfil within an adequate period of time the legal requirements of the FIU, supervisory authority and authorities in charge of criminal proceedings related to the customer and the financial operation.

Records on the riskiness of the customers

A subject of preservation are specific questionnaires related to the assignment of customers to groups by the riskiness of their activities or operations. Any important information, which confirms the circumstances justifying the assignment of a customer to a different risk group (thereby a change of his risk profile), acquired by communication with the customer or otherwise, shall be recorded and preserved together with other data on the customer.

Records on financial operations

Internal regulations of the bank have to set the obligation of recording all financial operations performed for customers, in the bank's accounting and reporting. Records on financial operations, which document accounting items, are supposed to be archived in a form, which enables the FIU, the supervisory authorities, control authorities and bodies in charge of criminal proceedings to set up a satisfactory record and to verify the risk profile of each customer. Supporting records contain the customer's instructions related to the payments of the customer.

The bank archives the records on each financial operation conducted by the customer, including one-time operations and operations performed for customers that have not opened an account with the bank. In such a case, the time limit for preservation is the same as for the preservation of identification records and documentation.

Records on internal notifications of an UBO and reports on an UBO

The bank must preserve all reports on unusual activities of customers – both internal notifications of an UBO destined for the DP and reports on an UBO, which the DP has sent to the FIU.

If after assessing the relevant information and knowledge related to unusual activity of the customer the DP decided that the business operation was no UBO and sent no report to the FIU, the reasons of such a decision have to be also recorded and preserved together with the records on the corresponding business operation.

Records on performed education and training

The bank preserves records on performed training of the competent employees, which contain the date and content of the performed education and a description of the competent employee confirming that the competent employee has participated in the training and has acquainted himself with the bank's Program for protection against money laundering and terrorist financing and related internal regulations of the bank.

The form of preserved records, retrieval of records

Subject to data preservation are originals or, if applicable, photocopies of paper source documents and documentation, as well data saved in personal computers and mechanical media of electronic data. The time limits for preservation are the same irrespective of the form, in which those data are archived.

Due to the need of additional provision of data on customers and financial operations of customers, above all for the FIU and bodies in charge of criminal proceedings, it is important that the bank be able to retrieve the necessary source documents (documentation and media) with data or records without undue delay and, in the case of a started verification or investigation, preserve them even after the expiry of the legal time limit until the competent body announces that a further preservation thereof is not necessary anymore.

I. THE ENSURING, SYSTEM AND PERFORMANCE OF INTERNAL CONTROL

A system of control aimed at the fulfilment of measures for protection against money laundering and terrorist financing must work in a reliable way at the bank. The system of control is made up by the determination of control responsibilities at all levels of management and ensuring the performance of banking activities, as well as the performance of control activity by

- the supervisory board of the bank,
- members of the statutory body,
- the designated person (the deputy to the DP and the prevention unit),
- managerial employees,
- competent employees within the processing of instructions (financial operations) of customers and
- the internal control and internal audit unit, upon which the control of all units of the bank falls, including the DP and the prevention unit and the competent employees.

Control performed by the statutory body of the bank and by the supervisory board of the bank

It is based on generally binding legal regulations and internal regulations of the bank and results from the position in the hierarchy of the management system of the bank. Regularly, at least once a year, the statutory body of a bank and the head of the branch office of a foreign bank evaluates the effectiveness of the existing system – the concept for protection of the bank against money laundering, the Program and particular measures, including the activity of the competent units and employees.

Control activity of the DP and managerial employees

It results from the competences, duties and responsibilities of the DP and of each managerial employee and is being performed as a regular and ongoing activity of controlling the fulfilment of work duties of subordinated employees in the field of protection against money laundering and terrorist financing.

Internal control and internal audit

The bank's internal control and internal audit unit controls the fulfilment of compliance with the Program and internal regulations and procedures adopted by the bank for the purposes of protection against money laundering and terrorist financing, as well as the performance of duties

by the competent employees, managerial employees and by the designated person (the deputy to the DP and the prevention unit).
The performance of the control is supposed to focus on controlling

- the conduct of the corresponding degrees (levels) of customer diligence,
- the procedures for ensuring an up-to-date state of the acquired information on customers (verification),
- the assessment of particular financial operations, monitoring of customers, their financial operations and business relationships,
- the evaluation and management of risks,
- the internal notification of an UBO and the reporting of an UBO to the financial intelligence unit,
- the conduct of training of employees and
- the preservation of records.

The control procedures and the type and extent of the resulting information serve as source information for verifying whether the bank‘s measures for protection against money laundering and terrorist financing are sufficient.
The statutory body should be informed on the results of the performed controls and audits at regular intervals, e.g. twice a year and, if serious deficiencies are detected, without delay.

In addition to controlling activities focusing on compliance with day-to-day routine activities by the employees of the bank at the individual workplaces at the headquarters, as well as in the network of branch offices of the bank, the whole system and process of prevention or protection of the bank against money laundering and terrorist financing, too, has to to be subject to an internal audit. The internal audit is supposed to evaluate the functionality, effectiveness and efficiency of all elements, instruments, procedures and managing and controlling mechanisms applied by the bank in this field.
This type of internal audit should be performed in accordance with the plan of activities of the internal control and internal audit unit with a periodicity resulting from an evaluation of the riskiness of the individual fields of activity of the bank. Due to the risk of loss of the bank’s credit associated with undesired participation in money laundering and terrorist financing, it is appropriate that this type of internal audit be performed at least once per a calendar year.

CONCLUSION

Methodological Instruction of the Financial Market Supervision Unit of the National Bank of Slovakia of 19 December 2008 No. 7/2008 for protection of a bank and branch office of a foreign bank against money laundering and terrorist financing is repealed.

Ing. Martin Barto, CSc. m.p.
The Vicegovernor

Annex

EXAMPLES OF UNUSUAL BUSINESS TRANSACTIONS

1. Money laundering through cash transactions

(a) Unusually high amount of cash deposits made by a natural person or legal entity in such business activities that would normally involve the use of cheques and other instruments.

(b) Significant increase in the amount of cash deposits made by a natural person or legal entity without any obvious reason, especially if such deposits are shortly transferred from their account and/or to a destination which is not normally connected with the client.

(c) Clients making cash deposits by using many cash deposit forms so that the amount of any such deposit is insignificant but the overall amount of all deposits is high.

(d) Accounts of a legal entity whose business operations, such as deposits and withdrawals, are realised in cash rather than by way of a debit or credit, which form is usually used by business corporations (e.g. cheques, letters of credit, bills of exchange, promissory notes, etc.).

(e) Clients who each time make cash deposits to cover bank bills of exchange, cash transfers or other negotiable and liquid cash instruments.

(f) Clients asking for the exchange of a large number of banknotes of a low nominal value for banknotes with a greater nominal value.

(g) Frequent exchange of cash money for other currencies.

(h) Branches having a lot more transactions in cash than usual.

(i) Clients whose deposits contain false banknotes or forged documents.

(j) Clients transferring high amounts of money abroad or from abroad with the use of cash payment orders.

(k) High cash deposits through night deposit box services, which enables avoiding direct contact with bank employees.

2. Money laundering through bank accounts

(a) Clients wishing to possess many holder or client accounts which are apparently not related to the kind of business, including business transactions, in which the administrators of the holder accounts engage.

(b) Clients who possess many accounts and deposit cash in each of them under such circumstances under which the aggregate sum of the deposits represents a high amount.

(c) Any natural person or legal entity whose account does not show any standard activities of a private account or corporate banking, but is used to receive or disburse high amounts that have no obvious purpose or relation to the account holder and/or his firm (e.g. considerable increase in account transactions).

(d) Clients holding accounts in several financial institutions in the same region, especially when the bank is aware of the regular consolidation of funds from such accounts before an order of transfer of such funds is given.

(e) Matching the transfer orders with the cash deposited in the account on the same or previous day.

(f) Depositing third party cheques issued in a high amount that are endorsed in favour of the client.

(g) High cash withdrawals from an account that was dormant/ inactive in the past or from an account to which an unexpected high deposit has been just credited from abroad.

(h) Clients who are jointly or concurrently using different bank counters to realise large business transactions in cash or foreign exchange transactions.

(i) Frequent use of safe deposit box services. Increased activity on the part of natural persons. The parcels that are placed inside or taken out are sealed.

(j) Representatives of legal entities avoid contact with the branch.

(k) Significant increase of cash deposits or negotiable securities by a legal entity using the accounts of another client or internal accounts of the company or holder accounts, especially when the deposits are immediately transferred between another company of the client and the holder accounts.

(l) Clients who refuse to provide information on the basis of which they could obtain a credit or other bank services under common circumstances.

(m) Insufficient use of standard bank services, e.g. avoiding services with high interest rates for a high balance.

(n) A large number of persons making payments into the same account without reasonable grounds.

3. Money laundering through banking activities

(a) Use of letters of credit and other methods of financing a business deal to transfer money between countries in which such business deal is inconsistent with the client's ordinary business activities.

(b) Clients who regularly make large payments, including bank transactions that cannot be clearly identified as transactions in good faith, into countries that are commonly associated with the production, processing or sale of drugs or with terrorist organisations or which regularly receive large payments from such countries.

(c) Significant account balance increase that does not correspond to the known turnover of the client's company and subsequent transfer into an account (accounts) abroad.

(d) Unexplained electronic transfers by clients of funds from/into an account or without employing an account.

(e) Frequent requests to issue traveller's cheques, bills of exchange in a foreign currency or other negotiable securities.

(f) Frequent depositing of traveller's cheques or bills of exchange in a foreign currency, notably if these originate abroad.

4. Money laundering through business transactions related to investments

(a) Purchase of securities that are to be kept in a financial institution's safe deposit boxes in instances when it appears to be inappropriate with regard to the client's apparent situation.

(b) Consecutive deposit/credit transactions with subsidiaries or branches of foreign financial institutions in regions known for illicit dealing in drugs.

(c) Clients' requests for investment (securities) management services if the source of funds is unknown or does not correspond to the client's apparent situation.

(d) High or unusual in-cash settlement of securities.

(e) Purchase and sale of a security without an obvious purpose or under circumstances that seem to be unusual.

5. Money laundering with the engagement of employees and intermediaries

(a) Changes in the employee's common behaviour, e.g. maintaining a costly lifestyle or avoiding a vacation.

(b) Changes in an employee's or intermediary's performance, e.g. a dealer selling products for cash has apparently or unexpectedly increased his performance.

(c) Any transaction with an intermediary when the identity of the beneficial owner or the counter party is kept secret in contradiction with the standard procedure applied to the particular type of transaction.

6. Money laundering through secured and unsecured loans

(a) Clients who have repaid non-performing loans unexpectedly.

(b) An application for a loan against assets possessed by a financial institution or a third party where the origin of such assets is unknown or such assets do not correspond to the client's situation.

(c) If a client requests a financial institution to grant or secure funds where the source of the client's financial contribution to the business transaction is unclear, especially with the use of real property.

Important information and documents related to preventive measures against money laundering and terrorist financing are on the following web sites:

www.un.org
www.fatf-gafi.org
www.coe.int/moneyval
www.bis.org
www.amlcft.org
www.wolfsberg-principles.com
www.fsa.gov.uk
www.fdic.gov
www.c-ebs.org

Contacts:

National Bank of Slovakia

- Licencing and Enforcement Department:	phone No. 02 5787 2873, 02 5787 2883
- Supervisory Department:	phone No. 02 5787 2834

Ministry of the Interior of the Slovak Republic, Financial Police Intelligence Unit:

phone No. 09610 514 05
09610 514 02
0905 962 815

Ministry of Finance of the Slovak Republic: phone No. 02 5958 2520