

**Guidelines to Recommendation No. 3/2008 (of November 20)  
of the Supervisory Council of the Hungarian Financial Supervisory Authority  
on the Prevention and Deterrence of Money Laundering and Terrorist Financing**

## **1. Introduction**

### **1.1. The harm caused by money laundering and terrorist financing**

Public perception, both domestic and international, considers money laundering as a serious violation of the law. Despite this certain market participants are occasionally forgiving when adjudicating incomes and wealth generated through the violation of taxation statutes and incomes generated from “smaller” bribes, and primarily emphasise the obligations of the financial organisation in providing services and the profit concerns that are important to its owners.

The owners of illegal incomes frequently attempt to engage in money laundering and terrorist financing using financial organisations that are forgiving and “flexible”.

The acceptance of doubtful and suspicious customers and transactions and the execution of such transaction orders are expressly harmful for financial service provider organisations. Getting entangled in the suspicion of money laundering and terrorist financing carries reputational and operational risks and may lead to a loss of markets.

Money laundering has by now become one of the most profitable and grandest scale businesses in the world. According to the IMF the volume of money laundering amounts to 2-5% of the combined GDP of all countries of the Earth. Expressed in specific amounts this represents at least USD 590-1,500 billion per annum.

Linked to organised crime, money laundering fundamentally distorts the functioning of the market and devalues the efficiency and integrity of financial procedures. Money laundering is not aimed at the realisation of profits, but merely at rendering the illegal sources of funds unrecognisable. Through terrorist financing funds from legal and/or illegal sources reach individuals or groups that perpetrate terrorist acts. The deterrence of the laundering of incomes generated from crime and especially from organised crime and the deterrence of terrorist financing is a central issue for the security of the entire economy, of the financial system, of financial organisations and their customers.

By presenting – in the course of their customer contacts – the harm caused by money laundering to individuals and to society as a whole, financial organisations and their professional associations can facilitate a negative social opinion for all forms of money laundering and terrorist financing.

International organisations such as the UNO, the Inter-Governmental Action Group against Money Laundering and Terrorist Financing, the Financial Action Task Force (hereinafter referred to as the FATF), the European Union, as well as the Council of Europe and its expert committee MONEYVAL, the IMF, the World Bank and the Basel Committee on Banking Supervision together with the IOSCO and with the IAIS treat national and international efforts for the prevention and deterrence of money laundering and terrorist financing as issues of emphasised significance. Member states were obliged to implement and enact Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the

prevention of the use of the financial system for the purpose of money laundering and terrorist financing (hereinafter referred to as the Directive) until December 15, 2007.

The aim of the Directive is to transpose the 40 recommendations of the FATF expressed in connection with the fight against money laundering into Community law. Another important aspect is to extend the scope to include terrorist financing in addition to money laundering, and to transpose the anti terrorist financing elements of the 9 special recommendations accepted by the FATF also into Community law.

The Directive was transposed into domestic law with the creation of Act CXXXVI of 2007 on the prevention and deterrence of money laundering and terrorist financing (hereinafter referred to as the Money Laundering Act: MLA) and with the required amendment of the related statutes.

The legal environment for the prevention and deterrence of terrorist financing was expanded with Act CLXXX of 2007 on the implementation of financial restrictive measures and the freezing of assets as ordered by the European Union and on the related amendment of certain Acts, with the aim to order the freezing of the economic resources and the financial assets of natural and legal persons and other groups and organisations on account of terrorism.

## **1.2. The fundamental documents of the fight against money laundering and terrorist financing**

The effective fight against money laundering and terrorist financing is only possible in the framework of international cooperation.

The action taken by international financial organisations and countries with developed economies against money laundering and terrorist financing to fight unlawful activities that are becoming increasingly complex and also employ cross-border services, justifies the procedures and methods facilitating the prevention and deterrence of money laundering and terrorist financing to be asserted more efficiently in the regulation and in the domestic practices employed. The international community has developed a broad system of standards in this regard, which is not evadable for the financial sectors of countries that have joined the international cooperation.

Special attention is to be paid to the following:

- To the 40 recommendations of the FATF;
- To the 9 special recommendations of the FATF against terrorism;
- To the Guideline prepared by the FATF for financial organisations on the detection of terrorist financing;
- To the FATF publication entitled: "Combating the abuse of non-profit organisations. International best practices.";
- To the explanations to the FATF recommendations and to the related best practices;
- To the FATF Report on Money Laundering Typologies published annually;
- To the Explanatory Memorandum of the European Union for the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000);
- To the recommendation of the Council of the European Union of 25 April 2002 on the improvement of investigation methods for the detection of organised drug trafficking and the financial affairs of drug traffickers;
- To the first, second and third anti money laundering Directives (Numbers 1991/308, 2001/97 and 2005/60) of the Council and of the Parliament of the European Union;

- To Council Directive 2006/70/EC of 1 August 2006 on the specification of implementation measures for Directive 2005/60/EC of the European Parliament and of the Council, with regard to the concept of “politically exposed persons” and to the technical requirements for simplified customer due diligence measures and for exemptions provided on the basis of financial activities conducted on an ad-hoc or highly restricted basis;
- To Publication No. 85 of 2001 by the Basel Committee on Banking Supervision and to the IAIS 2002 Guideline of January 9;
- To the joint publication of June 2003 issued by the Basel Committee on Banking Supervision, by the IAIS and by IOSCO on money laundering;
- To the Homepage of the UN Counter Terrorism Committee (UN CTC);
- And to the Wolfsberg Statement of large international private banks of October 2000 and January 2002.

The HFSA urges the domestic application of international rules and procedures that make the practices of financial service providers more reliable and more efficient for the prevention and deterrence of money laundering and terrorist financing. The HFSA continues to promote the cooperation of domestic organisations responsible for and interested in the action against money laundering and terrorist financing and the continued improvement of the activities of supervised institutions in this field.

### **1.3. Definition of money laundering**

The effective domestic regulations against money laundering are contained in the Penal Code and in the MLA. The Penal Code currently addresses two factual situations in relation to money laundering. The criminal regulations define the crimes as “money laundering” and “failure to comply with reporting obligations in connection with money laundering”.

#### **1.3.1. Definition of money laundering on the basis of the Penal Code:**

Article 303 Paragraph (1): A person shall be guilty of a crime and punishable by up to five years of imprisonment, if in order to conceal the origins of an asset originating from an act of crime punishable by imprisonment perpetrated by someone else, he/she:

- a) Transforms or transfers such an asset or uses it when exercising economic activities;
- b) Keeps secret or conceals a right to such an asset or any changes to such rights or the place where such an asset is to be found;
- c) Or performs any financial activity or uses any financial service in connection with such an asset.

(2) A person shall also be punishable pursuant to Paragraph (1) if he/she:

- a) Obtains for him-/herself or for a third person an asset originating from an act of crime punishable by imprisonment perpetrated by someone else;
- b) Keeps, handles, uses or utilises such an asset or uses it or its value to acquire other material assets;

If at the time of perpetration he/she was aware of the asset’s origin.

(3) A person shall also be punishable pursuant to Paragraph (1) if in order to conceal the origins of an asset originating from an act of crime punishable by imprisonment perpetrated by himself/herself, he/she:

- a) Uses such an asset while exercising economic activities, or;
- b) Performs any financial activity or uses any financial service in connection with such an asset.

(4) The sentence shall amount to between two to four years of imprisonment if an act of money laundering specified under Paragraphs (1) to (3) is perpetrated:

- a) In a businesslike fashion;
- b) For an especially high value or above;
- c) By an officer or employee of a financial institution, an insurance company, an investment service provider, a service provider on the commodities exchange, an investment fund manager, a venture capital fund manager, an organisation performing activities on the stock exchange or as a clearing and settlement house or as a central depository agent, a voluntary mutual insurance fund or private pension fund, or an organisation that organises gambling;
- d) By an official person; or
- e) By an attorney.

(5) A person who agrees to commit an act of money laundering as specified under Paragraphs (1) to (4) is guilty of committing a misdemeanour and is punishable by up to two years of imprisonment.

(6) A person shall not be punishable for an act of money laundering as specified under Paragraphs (1) to (5), if he/she voluntarily reports it to the authorities or initiates such reporting, provided that the act has not yet, or has only partially been discovered.

Article 303/A Paragraph (1): A person shall be punishable by up to two years of imprisonment, public labour or a fine for a misdemeanour if he/she:

- a) While exercising economic activities uses an asset originating from an act punishable by imprisonment perpetrated by someone else, or;
- b) Performs any financial activity or uses any financial service in connection with such an asset,

If out of negligence he/she was not aware of the asset's origin.

(2) The sentence shall be up to three years of imprisonment for a misdemeanour if an act specified under Paragraphs (1) is perpetrated:

- a) For an especially high value or above;
- b) By an officer or employee of a financial institution, an insurance company, an investment service provider, a service provider on the commodities exchange, an investment fund manager, a venture capital fund manager, an organisation performing activities on the stock exchange or as a clearing and settlement house or as a central depository agent, a voluntary mutual insurance fund or private pension fund, or an organisation that organises gambling;
- c) By an official person.

The legal object of the crime is an interest in the legal functioning of the financial sector and in the successful fight against organised crime. The crime is perpetrated with regard to an asset. In a legal sense asset includes anything that could be the object of proprietary rights. Thus, the concept of asset is to be interpreted in the broadest possible sense. The asset mentioned in the factual situation must originate from the perpetration of an act punishable by imprisonment. It is not necessary for the underlying case to have been completed with a legally binding sentence.

### **1.3.2. Failure to comply with reporting obligations in connection with money laundering**

Pursuant to Article 303/B (1) of the Penal Code a person who fails to comply with reporting obligations as prescribed by the Act on the prevention and deterrence of money laundering

and terrorist financing is guilty of committing a misdemeanour and is punishable by up to two years of imprisonment.

As a second step in the prosecution of money laundering under criminal law, the legislator provides for punishment also for failure to comply with the reporting obligations. The description of the factual situation in the law is a skeleton statute, with its actual substance provided by the MLA.

### **1.3.3. The progress of money laundering through the financial system**

The most widespread concept of the phases of money laundering is the three-phase model. According to this concept the process of money laundering is usually subdivided into three sections, the process however does not necessarily progress through all of the three phases. The classic flow diagram contains the stages of placement, layering and integration.

- Placement (and separation): The cash is separated from the underlying crime and is transferred to financial organisations. The money originated from crime is usually taken by the criminals to banks, from where they transfer it within a short time to another bank and exchange it into other means of payment. Criminals often use unknown and unsuspecting persons with no criminal records to deposit the money obtained through crime in small batches into banks and they pay their collaborators well for this. The principals exercise strict control to ensure that collaborators proceed as instructed and to ensure that the money arrives at the destination according to their instructions. The identity of the principal remains concealed even if the collaborator executing the deposit is identified. A method employed for money or a valuable asset obtained abroad through crime is to transfer it across the border (by way of an electronic transfer or physically) as if it was revenue generated from lawful standard business activities in orderly management. To facilitate placement, criminals mix “dirty” incomes waiting to be “laundered” with the cash revenues of businesses with large cash turnovers (such as casinos and other forms of gambling, department stores, restaurants, money exchange booths, etc.). By establishing cover enterprises they hide their capital originating from crime behind nominal owners (and executives) that operate fully in compliance with the laws and other legal statutes, and withdraw their profits thus generated as lawfully taxed income.
- Layering (hiding): Within this stage illegal incomes are separated from their sources, revenues are concealed so that it becomes impossible to discover the connection between the person obtaining the income and the money originated from crime. The source of the money is rendered untraceable with the use of crossing and covering transactions, purchases, electronic transfers and multiple transfers. Legal titles are created employing international off-shore corporations and financial organisations and using fake and fictitious invoices, contracts and international trade documents. There are cases where phantom corporations and individuals existing only on paper are used in order to fulfil obligations that are presented as real.
- Integration, legalising: During this phase the funds originated from crime are returned to the economy and are indicated as funds from legal business sources, which thus appear as funds originating and arriving at recognised financial organisations. The funds originated from crime are integrated into a legally established enterprise and are indicated there as revenue, book-keeping data is

falsified on both the revenue and expense sides and “laundered” money is covered with fictitious invoices. (E.g., the shop or the restaurant presents a sales turnover which is greater than the actual and the sums awaiting laundering are placed into the variance.)

### **1.3. 4. Terrorist financing**

As a consequence of the international legislative process the issue of terrorist financing is increasingly discussed together with money laundering and in comparison to money laundering has the following differentiating features:

The motive of terrorism is more violent (to intimidate) than material (the desire for profits). The aim of terrorists is mostly to force state organisations and international organisations to do something, to intimidate the population or to change (or to disturb) the constitutional, social or economic order of another state.

The third differentiating feature is the difference in the sums involved. Even larger terror attacks can be organised and executed using small sums of money, while money laundering, due to its nature, is usually perpetrated only for larger sums.

The objectives described by international documents are also contained in the Hungarian Penal Code in Article 261 on acts of terror.

Blocking the sources of funds for terrorism is a condition of accentuated importance for the deterrence of terrorism. Terrorists collect illegal funds and funds that seem legal in character: in addition to protection moneys, blackmail and trading in drugs and weapons they also collect funds from legally functioning foundations and non-profit organisations and also collect membership fees and sell publications. In order to carry out these activities:

- They use cover companies that operate regularly, the revenues of which are intermixed with their dirty funds;
- They use pretence firms that perform no substantial activities and serve only to conceal the owners and the assets of the firm;
- They use informal monies and systems for funds transfer (Hawala);
- They use front men;
- They place cash or purchase securities in large amounts, but always under the limit for reporting at any single time;
- They use credit cards in ATMs, thus converting credit into cash;
- They smuggle cash from one country to another.

The FATF has issued its Nine Special Recommendations with the aim to prevent and deter terrorist financing. In the year 2002 the European Union condemned terrorism in a skeleton resolution and stated the following: “The European Union relies on the foundation of the universal values of human dignity, freedom, equality and solidarity and respect for human rights and fundamental freedoms and relies on the principles of democracy and the rule of law professed jointly by its member states. Terrorism is one of the most severe violations of these principles.”

The Directive creates a strong connection between the issues of money laundering and terrorist financing. Responsibilities in customer due diligence and reporting are to be carried out in a uniform system and service providers carry the burden of reporting obligations not

only for data, facts or circumstances indicative of money laundering, but also for data, facts or circumstances indicative of terrorist financing.

The procedures to recognise the intent of money laundering are to be employed also to deter terrorist financing, with special regard to cases where the sums being moved are small, but where both their purposes and legal titles are uncertain. Service providers may have doubts frequently as to the senders and addressees involved.

### **1.3.5. Definition of facts, data and circumstances indicative of money laundering and terrorist financing**

It becomes necessary to define facts, data and circumstances indicative of money laundering and terrorist financing for all transactions that are inconsistent with the account history or the previous regular business habits and practices of a known customer, with the peculiarities of the turnover of the account maintained by the service provider, with the movements of funds in connection with a transaction, and where there are no known or acceptable reasons for the inconsistencies, and where the transaction could be suitable to perpetrate money laundering and terrorist financing. The definition of facts, data and circumstances indicative of money laundering and terrorist financing is not identical to the terminology of suspicion used by Act XIX of 1998 on Criminal Proceedings.

Among others attention is needed:

- To see whether or not the size of the specific transaction is consistent with the usual activities of the customer;
- To see whether or not the transaction is reasonable based on the previous business and personal practices of the customer;
- To see whether or not the transaction initiated by the customer indicates a change consistent with the previous practice, or whether or not it deviates from it;
- If there are outward and inward cash payments on the same day or within a short time interval without actual cash movements where the transaction involves the accounts of several customers;
- If a current account overdraft is provided within the day which is transferred as a single sum without real economic content to closed companies that are in proprietary and funding relationships with each other and where at the end of the day the sum returns to the bank account of the company that has initiated the transfer;
- To see whether or not the features of dormant accounts, the sizes of deposited funds and the circumstances of a “sudden awakening” indicate anything unusual and whether or not they provide a reason for suspicion;
- To see whether or not the customer has a palpable reason to involve a third country in the case of a cross-border transaction order;
- To see the reason for a guarantee provided where it is not possible to demonstrate any relationship between the debtor and the guarantor;
- To see whether or not the turnover of the money exchange bureau holding the account conducted in domestic and foreign currencies is realistic and whether or not it is conducted in the usual currencies and volumes;
- To see whether or not insurance brokerage and brokerage assignments are used to legalise illegal incomes by way of insurance contracts;

- To see if the termination of an insurance contract or fund contract is reasonable and explicable on the basis of the known circumstances of the insured or of the fund member;
- If the contracting and the insured parties are not identical persons in the case of life insurance contracts for high amounts;
- To see whether or not the circumstances for the contracting and premature repurchase of unit-linked life insurance contracts are reasonable from an investment point of view.
- If a partial repurchase of a unit-linked life insurance investment is not paid to the specified usual bank account;
- If there are continued inward payments for palpably loss-making investment and unit-linked insurance contracts and accounts;
- To see whether or not an inward payment to the account of the insured (fund member) arrives from the usual institution or person, or if unexpectedly an unknown third person makes a payment for a more significant amount;
- If VIP customers transact insurance and investment transactions for especially large sums and high values;
- When contracts for high sums with one-time premiums are made or unreasonably terminated;
- If the representatives of business organisations appear in person at the financial organisation only when opening their accounts and subsequently conduct transactions only electronically, and if their contact details include only their foreign (off-shore) seats and mobile phone numbers.

## **2. Institutional regulations and procedural rules for the fight against money laundering and terrorist financing**

### **2.1. Internal regulations**

Service providers governed by the MLA are obliged to prepare practical internal regulations for the prevention and deterrence of money laundering and terrorist financing. The required sample regulations and guidelines are freely downloadable from the homepage of the HFSA.

Service providers shall establish and operate their internal procedural rules in connection with the prevention and deterrence of money laundering and terrorist financing, and the individual elements and duties constituting parts thereof, with consideration to the relevant statutory provisions and consistently with the peculiarities, extent, complexity and risks of the activities conducted by the service provider institution.

Internal regulations are approved by the HFSA if they include the mandatory substantial elements as described in the decree for the execution of the MLA and if they are not in conflict with any legal statutes.

### **2.2 Designated Person (Money Laundering Reporting Officer, MLRO)**

Service providers shall designate a person – one or more depending on the size of the firm – to forward any reports against money laundering and terrorist financing to the authority operating as the financial intelligence unit.

The responsibility of the designated person is primarily to forward reports without delay to the authority operating as the financial intelligence unit, and beside this to participate in

organising the training of employees and to lead the fight against money laundering and terrorist financing.

The designated person or a person obligated for this by the service provider shall make sure that the control mechanisms are created and operated. Transactions screened in monitoring are to be analysed and those in relation to which data, facts or circumstances emerge indicative of money laundering or terrorist financing are to be reported without delay by the designated person.

If possible the designated person should be a senior employee of the service provider with regard to the accentuated significance of his/her responsibilities. If the institution has no separate manager responsible for compliance with the rules, the designated person should be a senior employee of the service provider whose working hours are to be specified to enable his/her or his/her deputy's continued availability to employees for consultation and reporting.

It is recommended for the designated person to regularly inform the management of the firm, the internal audit function and the supervisory committee of his/her activities.

### **2.3. Customer due diligence**

Service providers are obliged to employ customer due diligence measures when establishing a business relationship. For customers with whom the service provider has not previously established a business relationship, due diligence is to be carried out when the value of a transaction order or of several de-facto related transaction orders initiated by the customer reaches or exceeds the limit sum of three million six hundred thousand Hungarian Forints, or if when changing money the value of the transaction reaches or exceeds five hundred thousand Hungarian Forints. Service providers are obliged to carry out due diligence measures on their customers if some data, facts or circumstances emerge that indicate money laundering or terrorist financing if due diligence measures were not yet performed. Service providers are also obliged to carry out customer due diligence measures if there are doubts as to the veracity or adequacy of the customer identification data previously recorded.

In the mentioned cases of the obligation to carry out customer due diligence measures service providers shall identify the customer and shall verify his/her personal identity, and shall also identify the beneficial owner and verify the personal identity of the beneficial owner if there are doubts as to the personal identity of the beneficial owner. In addition to the above, service providers shall also record the details of the business relationship and the transaction order and shall perform continuous monitoring of the business relationship.

Service providers are entitled to specify the extent of such customer due diligence measures on a risk-sensitive basis. In this context the MLA specifies minimum and maximum data sets for the identification of customers and of beneficial owners as well as for recording the details of business relationships and of transaction orders.

The provisions of the MLA governing customer due diligence differentiate between regular, simplified and enhanced due diligence procedures.

### **2.4. Risk based approach to customer due diligence measures**

Pursuant to the risk based approach the system prescribing an identical procedure for all customers has ceased to exist. Service providers may now specify on a risk-sensitive basis the extent of their due diligence measures depending on the customer, the business relationship, the product or the transaction type.

Relying on the risk-based approach the MLA specifies two versions for customer due diligence in relation to the base case, i.e., simple and enhanced customer due diligence. Consistently with the requirement of the risk-based approach service providers record minimum and maximum data sets for the identification of customers, for the identification of beneficial owners and for recording the details of business relationships and of transaction orders. Service providers shall classify their customers and transactions accordingly. It is recommended for data entry into the information technology system to be performed independently of the minimum and maximum data sets, managed in a uniform fashion that allows easy and rapid retrieval.

Customer due diligence on a risk-sensitive basis may not be construed to treat all transactions and business relationships as representing an enhanced exposure to the risk of money laundering and terrorist financing and thus for service providers to employ enhanced customer due diligence procedures for all cases and to identify all customers using the maximum data set. From a prudential point of view it is therefore not acceptable to employ a procedure pursuant to which service providers employ the enhanced customer due diligence procedure in all cases.

## **2.5. Prudence in customer management**

In order for the prevention and deterrence of money laundering and terrorist financing to be successful and efficient, service providers should employ prudence when establishing business relationships with their customers and when executing transaction orders, and also throughout the entire existence of the business relationship.

Based on the recommendation of the Basel Committee for Banking Supervision service providers are to develop an accepted and regular practice from the requirement to act with prudence in getting acquainted with their customers. Regardless of whether relationships are initiated by customers or by service providers, service providers should act with prudence in assessing the situation of their customers and the nature of their business habits and activities.

Special care is necessary in examining customers that move over from other credit institutions or financial service providers to use identical or similar services. It is expedient to inquire about the reason for the change and if possible to request information from the customer's previous bank, in a way acceptable within interbank relations. It is also expedient to do the same when a customer changes bank branches but not banks, and uses services not previously used (such as investment services or telephone banking or internet banking services).

Prudent inquiry is necessary of the intentions and situations of customers especially when contacts are not initiated in person, but through the use of otherwise authorised intermediaries, consultants, attorneys or asset managers.

Service providers should develop internal substantial and technical requirements in order to prudently acquaint themselves with their customers. They should keep in mind that it is in the

interests of both the service provider and the customer to establish trust based on mutual acquaintance.

## **2.6. Know your customer - KYC**

In order to mitigate the risk of money laundering and terrorist financing, within the course of their regular and active relationships with their customers service providers should understand to the greatest possible extent the substance of the activities of their customers, the nature of their business relationships, their circle of partners, financial habits, domestic and international market practices, as well as the origins, currencies and usual magnitudes of their executed debits and credits.

Service providers must know the ownership structures of their legal entity customers inclusive of their beneficial owners who may only be natural persons and must know their executive managers with decision making powers and the persons authorised to act in the name of the customer vis-à-vis the service provider in ways agreed with the service provider.

Service providers must require their customers to provide timely and appropriate information to the service provider on internal changes that are expected or have already occurred.

Special attention must be paid to well known customers who are public figures whose irregular financial conduct, if any, could also damage the reputation of the service provider. The responsibility for relationships established with such customers should rest with a senior manager.

For deposits made by attorneys or notaries public, financial organisations should obtain declarations of the beneficial owners from their customers making the deposits.

## **2.7. Customer profile**

Service providers shall create customer profiles on the basis of their customer due diligence measures and their prudent acquaintance of their customers, on the basis of the systematisation of their business, financial and payment habits, and on the basis of appropriate records of their relationships and turnover of funds. Pursuant to the MLA service providers shall record data on business relationships and transaction orders and shall continuously monitor their transaction relationships. In order to establish these customer profiles service providers shall compile a standard questionnaire or shall use an assessment system with appropriate parameters, and shall rely on these in preparing the customer profiles, which they shall regularly review.

These profiles can ensure the transparency and lucidity of customer transactions and their relationships at all times. Relying on the established customer profiles it will be possible to assess and elucidate irregular events and irregularity. Thus it will be possible to determine with speed and security if a disruption or irregularity occurs in the habits or in the turnover of a specific customer.

## **2.8. Declaration on the beneficial owner**

The rules related to beneficial owners require service providers to know, in addition to the customer, the beneficial owner, who is the ultimate owner of the customer that is a legal

entity or a legal arrangement, or who ultimately controls it and/or the natural person on whose instructions a certain transaction is executed or who is a beneficiary of such. Only natural persons can be beneficial owners.

International practices and regulations also extend to asset management companies and thus it is recommended for service providers to strive to know these legal entities as well.

In order for service providers to be clear at all times about the identities of the persons in whose interests and on whose instructions they conduct their executed operations, in the course of customer due diligence service providers shall obtain written declarations from their customers on whether the transaction orders are carried out in their own names or in the names of others. The law mandates the person taking the action to make such a declaration. Such a declaration is always to be made by the natural person taking action as to whether the transaction is carried out using his/her own assets or whether he/she is taking action in the interests of some other natural person or legal entity.

If the written declaration made by the customer for the service provider states that he/she is proceeding not in his/her own name but in the name or in the interests of the beneficial owner, then the written declaration must include the details of the beneficial owner as specified in the MLA. If there are doubts as to the authenticity of the declaration on the beneficial owner, it is then to be verified.

In view of the requirement for customers who are legal entities to be examined in a way that enables the service provider to verify their incorporation and their registration in other certified public records and their ownership structures, and to be able to verify the identity of their beneficial owners, if these can't be identified from the documents presented, the service provider may then request further documents containing the details of the beneficial owners of customers that are legal entities or legal arrangements.

Even if the owner is represented by a proxy or by some other nominee, at least one person at the service provider should know the identity of the beneficial owner. The obligations to identify the beneficial owners of joint accounts maintained by notaries public or by attorneys include the obligation for the notaries public and attorneys to verify on their own the personal identities of the beneficial owners of the joint accounts that they manage.

The proxy or the customer should name the beneficial owner if he/she is not a customer of the service provider, using identification details that enable the identification of the beneficial owner without the possibility of him/her being mistaken for someone else. Accuracy is in the interests of both the customer and the beneficial owner, because the named individual may have to bear the inconveniences of being wrongly identified or mistaken for some other person who may for some reason be included on a list that gives rise to a reporting obligation.

## **2.9. Politically Exposed Person-PEP**

Politically exposed persons are natural persons who are residents of a foreign country and are or have been entrusted with a prominent public function, and their immediate family members or persons known to be close associates of such persons. Only foreign persons, i.e., persons who are residents of another member state or a third country and who qualify as such under the laws of their own countries shall be considered as politically exposed.

The MLA classifies politically exposed persons as customers subject to enhanced customer due diligence measures. Pursuant to this customers who are foreign residents shall in all cases

provide written statements to their service providers as to whether or not they qualify as politically exposed persons under the laws of their countries of residence, and in what capacity if yes. If there are doubts as to the authenticity of a declaration, it has to be verified.

There is no need to employ enhanced due diligence measures on domestic politically exposed persons. Service providers may subject such customers to due diligence measures according to the general rules on the basis of the principle of prudence in customer management.

The rules related to politically exposed persons have appeared not only because of the fight against money laundering but are also aimed at fighting corruption. Special attention needs to be paid to the financial conduct and habits of these customers also because any irregularities in connection with politically exposed persons may cause aggravated harm to the reputation of the service provider.

The risks in connection with politically exposed persons may be mitigated if the service provider develops internal policies and procedural rules for due diligence on politically exposed persons and if their accounts and transactions are separately monitored by the service provider, and furthermore if the service provider institutes records and lists allowed under legal statutes that enable it to identify politically exposed persons and to carry out their due diligence more simply and more efficiently.

## **2.10. Correspondent banking services**

Correspondent banking services are banking services provided by one bank (the “corresponding bank”) to another bank (the “corresponded bank”).

The correspondent banking accounts used by banks worldwide enable banks to close deals and to provide services that banks do not normally provide directly to their customers.<sup>1</sup>

Correspondent banking accounts that enable banks to provide services in countries where the corresponded banks are not physically present merit special attention. Financial institutions should employ prudence in customer management for such accounts to mitigate the risk of forwarding moneys linked to illegal activities.

Pursuant to the MLA and to international standards, a financial service provider shall accept orders issued within the framework of correspondent banking services only from service providers registered in third countries the internal procedures of which comply with the 40+9 recommendations of the FATF, and where the involved service provider has already carried out customer due diligence measures prior to the establishment of the correspondent banking relationship and has prepared a discovery analysis of the system of instruments employed against money laundering and terrorist financing. In addition, the service provider must have verified that the service provider with its seat in the third country has already carried out the verification of the personal identity of the customer with direct access to the correspondent account and continuously monitors the business relationship and is able to communicate the relevant customer due diligence data if requested. Financial service providers must deny the establishment or the continuation of correspondent banking relationships to corresponded banks registered in countries where they are not physically present and where they are not members of a regulated (i.e., supervised) financial group (so called “shell banks”).

---

<sup>1</sup> The obligations in connection with correspondent banking relationships apply to credit institutions.

Financial service providers must accordingly collect information on their corresponded banks to enable them to understand the nature of the businesses of the corresponded bank and to know the management of the corresponded bank, its significant business activities and its activities to explore and to prevent money laundering and terrorist financing.

Financial service providers must establish whether or not their corresponded banks have rules for “sufficient prudence” and whether or not they comply with those when managing financial operations conducted through correspondent banking accounts. They must be especially alert with regard to the risk that correspondent banking accounts could be used by a third party directly to conduct its own transactions through these accounts (so called payable-through accounts used by customers directly under the name of the institution).

### **2.11. Reporting in connection with incomplete information on the payer accompanying transfers of funds**

In order to step up against terrorist financing the FATF defines its expectations with regard to the forwarding of information on the payer accompanying transfers of funds in its special recommendation VII.

Relying on this and for the sake of community action the European Union has created its Regulation 1781/2006/EC on information on the payer accompanying transfers of funds, directly effective in its member states and setting forth the requirement for payment service providers to record information on the payer when transferring funds and to forward those together with funds transfers. The full set of information on the payer consists of the payer’s name, address and account number. The address of the payer may be substituted with his/her place and date of birth, while his/her bank account number may be substituted with his/her national identification number.

If both the paying and receiving financial institutions are located within the Community, it is sufficient to provide the account number of the payer or a unique identifier that enables the transaction to be traced back to the payer. The single piece of information specified in the Regulation becomes at least two in reality because transfers contain both the account number or the unique identifier and the name of the payer.

If instead of the at least three pieces of information on the payer a transfer is received with incomplete or missing information, then the Regulation prescribes such transfers to be refused or that the missing information be requested to be sent in addition. If problems with missing information are found to occur regularly then the service provider must consider terminating the correspondent banking relationship with the credit institution at fault.

The Regulation does not expressly prescribe a prohibition against the crediting of transfer orders that arrive with incomplete information and thus neither does a request for missing information to be sent mean that the crediting of the transferred funds should be suspended until the arrival of the missing information.

### **2.12. Customer due diligence measures carried out by another service provider**

A service provider may accept the outcomes of customer due diligence measures carried out by another financial service provider operating in the territory of the Republic of Hungary or in another member state of the European Union, or in a third country employing equivalent customer due diligence and record-keeping requirements as specified under Sections a) to e)

and l) of Paragraph (1) of Article 1 of the MLA, with the exception of service providers engaged in money transfer and money changing activities.

If the customer due diligence measures were performed by a service provider active in a third country, then such service provider must be listed in a mandatory trade register and must apply customer due diligence and record-keeping requirements as laid down in the Act or equivalent to those and must be subject to supervision according to the requirements specified in the MLA or equivalent to those or its registered office must be located in a third country that imposes requirements equivalent to those laid down in this Act.

The acceptance of the outcomes of customer due diligence measures carried out by another service provider requires customer consent because service providers require customer consent in order to share data with another service provider if requested for customer due diligence.

### **2.13. Procedure related to customers not fully identified**

Starting from 1 January 2009, the date prescribed in the law, service providers may not accept transaction orders from their earlier customers that have not appeared physically in person or via a representative at the service provider for the purpose of customer due diligence and for which the due diligence data and the declarations on the beneficial owner, pursuant to the MLA in effect since 15 December 2007, are not fully available. Customer due diligence measures may also be carried out by accepting the outcomes of due diligence measures carried out by another service provider, and not only if the customer appears physically in person or through a representative.

The refusal of a transaction relates not only to independent ad-hoc transaction orders but also to transaction orders issued within the framework of a long-term legal relationship. Following 1 January 2009 a business relationship may not be established and may not be maintained for a customer for which due diligence information is not fully available.

Service providers should review their existing clientele and if they find customers whose due diligence information is not fully available pursuant to the MLA, or whose declaration on the beneficial owner is not adequate, they should contact them in writing, or in some other way if not possible in writing, in order to enable their due diligence and in order not to have to refuse the execution of their transaction orders following 1 January 2009.

The official premises of the service provider are the most appropriate location for establishing personal contact. Nevertheless, in exceptional cases as set forth in the internal regulations and subject to strict conditions also as set forth in the regulations (such as the requirement for two employees for identification) it should be possible to carry out due diligence measures elsewhere, such as in hospitals or in retirement homes, for persons who are unable to visit the premises of the service provider through no fault of their own. For foreign customers it may be helpful to use the outcomes of customer due diligence measures performed by another service provider.

### **2.14. Screening system**

Pursuant to the MLA service providers are obliged to operate internal audit and information systems to facilitate customer due diligence, reporting and record-keeping in order to deter

business relationships and transaction orders that enable or implement money laundering and terrorist financing.

The legal obligation for the internal audit and information system should be demarcated from the monitoring activities carried out by the service provider, an obligation pursuant to which the service provider must continuously monitor the business relationship, including the analysis of transaction orders executed throughout the existence of the business relationship, in order to determine whether or not a specific transaction order is consistent with the customer data available to the service provider pursuant to legal statutes.

In order to fully comply with the legal obligation for monitoring, service providers should operate automatic screening systems relying on their existing information technology systems, to screen out unusual transactions from the account management systems and to forward those to the designated person for analysis. Organisations of smaller sizes or those with special activities may also operate their audit and information systems (screening systems) manually.

It is important for screening systems to enable appropriate parameter settings and subsequent improvements to avoid having to request costly program modifications for new perpetration methods, a process much slower and much more inflexible than if designated persons themselves could also enter new parameters into the systems. If possible, screening should extend to all transactions and should be able to recognise all techniques and transactions for money laundering and terrorist financing that have become known.

Service providers should pay special attention to money laundering and terrorist financing risks that may arise from the use of new or developing technologies and should take all measures that may be necessary to prevent their use through financial organisation systems.

### **2.15. Internal procedural rules for reporting**

Service providers are obliged to develop within their regulations internal procedural rules for reporting, wherein they should specify how and via what route reports are to be sent to the authority acting as the financial intelligence unit and how and where their copies and the related documents are to be kept. This is necessary in order to enable employees to adequately respond when detecting the emergence of data, facts or circumstances indicative of money laundering and terrorist financing.

Service providers detect irregularities, data, facts or circumstances indicative of money laundering or terrorist financing, but may not take action as investigative authorities. Service providers act appropriately if they examine the data, facts or circumstances indicative of money laundering and their causes and if they make reports on the basis of the real “reasons for suspicion” that emerge in the course of the examination. Based on the reporting made due to an irregularity it is the obligation of the authority operating as the financial intelligence unit to confirm or to reject the suspicion of money laundering and terrorist financing under criminal law. Reporting persons should strive to send the fullest possible data set in connection with the involved transaction.

Service providers should monitor the fate of their reports through their designated persons and should demand timely feedback. A report classified as unfounded does not mean that a repeated report is not to be made on the person upon the emergence of the next suspicion.

Business organisations whose representatives appear at the financial organisation only when opening an account and subsequently carry out only electronic transactions and whose contact details are provided only with the foreign (off-shore) seat of the company and with a mobile telephone number are used with increasing frequency to perpetrate both severe economic crimes and money laundering crimes. It is worthwhile for financial organisations to pay increased attention to the activities of such customers.

If some data, fact or circumstance emerges that indicates money laundering the manager or the employee of the financial service provider should carry out customer due diligence measures irrespective of the value threshold if not carried out earlier, and should without delay make a report on the emergence of the data, fact or circumstance indicative of money laundering or terrorist financing.

Starting from 15 December 2008 reports are to be forwarded to the authority operating as the financial intelligence unit exclusively in the form of protected electronic messages. Pursuant to this all service providers governed by the Act should be in possession of some electronic system as of 15 December 2008.

Up until the deadline indicated in the Act it is expedient for reports to be sent with return receipt or by facsimile in urgent cases, but it is recommended to also confirm the reporting on paper if it was sent by facsimile, but it is to be indicated in such cases that the paper report is a confirmation of a report already made by facsimile.

## **2.16. Suspension**

Pursuant to the MLA service providers must suspend the execution of transaction orders if some data, fact or circumstance emerges that indicates money laundering or terrorist financing in relation to a transaction order, and if an immediate action by the authority operating as the financial intelligence unit is deemed to be necessary in order to verify the data, fact or circumstance indicative of money laundering or terrorist financing. In such cases service providers are obliged to make a report without delay to the authority operating as the financial intelligence unit in order to enable it to verify whether or not the report is well founded.

Suspension and refusal to execute transactions for not fully identified customers both relate to transaction orders, which can be construed within a long-term legal relationship, i.e., within the business relationship on the one part, and independently of that as ad-hoc transactions on the other part.

## **2.17. Responsibilities of employees**

If some data, fact or circumstance emerges that indicates money laundering and terrorist financing employees must without delay prepare the data sheet for reporting and forward it to the designated person as specified in the service provider's internal regulations against money laundering and terrorist financing.

If at the time of reporting the data set on the customer or on the transaction was not sent in full in order to facilitate rapid information, it is reasonable to complete the supply of data within the shortest possible time, with special consideration to the related questions of the authority operating as the financial intelligence unit. Explanations are to be appended if necessary for the interpretation of the data contained in the documents sent in support of the reporting. Employees may consult with the designated person in the course of their actions. Employees are exempted from the obligation of secrecy in relation to reporting prescribed by the law and may not be sanctioned in any way for any reports found to be unfounded if they were made in good faith. Since the name of the reporting employee may not be indicated on the report, the identity of the reporting person is not directly available to the authority operating as the financial intelligence unit which can only maintain relationships to such employees via the designated persons, meaning that employees can make anonymous reports.

The following may substantiate the suspicion of money laundering:

- Something unusual, if there is an unexpected change to the hitherto demonstrated financial conduct of the customer that can't be explained with business or financial causes;
- Something unusual, if unexpectedly a new person or business and geographic area inconsistent with the customer's regular practices appears within the customer's known business and financial networks;
- Something unusual, if the transaction is not consistent with the practices employed by the customer due to the uniqueness of the transaction or due to the use of an unusual payment method;
- Something unusual, if the intended sum of the transaction seems to be as usual but if it is intended for a purpose that is different from and less credible than those normally recognised;
- If the explanation for the transaction seems to be artificial;
- If on the basis of the circumstances it is probable that the involved sum originates from a crime;
- Operations related to off-shore financial organisations;
- Unusual credit transactions and unusual cross-border funds movements;
- Investments in real estate and other investments without an obvious economic purpose;
- The appearance of deviations from reported business activities and business relationships and anomalies in the sizes and routes of funds movements and in customer relationships;
- If customers intentionally provide incomplete information and if they withhold important data, if there are intentional inaccuracies in relation to transaction orders.

Annex No. 2 contains the typology, organised into a uniform structure, of unusual transactions observed hitherto by the profession and affecting the operations of all service providers governed by the MLA, which could provide the basis for data, facts or circumstances indicative of money laundering or terrorist financing, i.e., for reporting.

## **2.18. Responsibilities of superiors**

If internal regulations prescribe information to be provided also to the direct superior, it is then expedient for the direct superior of the employee to verify whether or not additional data is available for the reporting. Should the superior deem it justified to append additional data, it is to be sent as a supplement to the reporting.

### **2.19. Responsibilities of the designated person**

If the institution has no separate manager responsible for compliance with the rules, the designated person should be a senior employee of the service provider whose working hours are to be specified to enable his/her or his/her deputy's continued availability to employees for consultation and reporting. Not later than when receiving its operating license the financial organisation is obliged to register with the authority operating as the financial intelligence unit, i.e., to inform the authority operating as the financial intelligence unit of the designated person's name, position and telephone number. The authority operating as the financial intelligence unit should indicate its own administrator and contact details within its response. Upon a change the financial organisation is obliged to inform the authority operating as the financial intelligence unit within five days about the details of the new designated person. The name of the designated person, and where possible, of his/her deputy are to be stated also in the regulations together with their direct contact details, to enable employees to make their reports. It is expedient for the designated person to also verify reports with regard to form and substance. It is the responsibility of the designated person to provide training to employees or to organise training for employees at least once every year.

### **2.20. The compliance organisation and internal audit**

Larger service providers (with emphasis on credit institutions and insurance companies) shall create separate compliance functions in view of Recommendation No. 11/2006 issued by the Supervisory Council on the establishment and operation of internal lines of defence. Article 21 of the Act on Investment Service Providers mandates the use of compliance officers for investment firms. The compliance function includes in specific the prevention and deterrence of money laundering and terrorist financing and the development and operation of KYC (Know Your Customer) and CDD (Customer Due Diligence) procedures.

The examinations carried out by the service provider's internal audit function must extend in particular to the following:

- Due diligence on customers who are natural persons, on the representatives of firms, on proxies and people with disposal powers;
- Recording of declarations on beneficial owners and examination of the completeness and sufficient detailing of reports;
- Compliance with the reporting obligations;
- Examination of the operation of the electronic screening system against money laundering and terrorist financing;
- Audit of the training on activities to fight money laundering and terrorist financing and of the related examination and audit of the service provider's agents with regard to their compliance with the rules of the MLA.

The compliance organisation shall report on its activities at least once every year to the service provider's supervisory board and to its management.

Neither the compliance officer nor the designated person may be members of the internal audit function because it is a violation of the independence of the internal auditor if he/she performs other duties in addition to his/her duties as an internal auditor, which would be inconsistent with prudent operation because two audit functions would be concentrated within a single hand.

If for the time being the service provider has no separate compliance function, its internal audit function may perform the regular audit, at least once every year, of its compliance with the regulations against money laundering and terrorist financing, and with the procedural rules on customer due diligence and reporting.

## **2.21. About the implementation of financial restrictive measures and the freezing of assets ordered by the European Union**

Pursuant to Act CLXXX of 2007 on the implementation of financial restrictive measures and the freezing of assets as ordered by the European Union and on the related amendment of certain Acts, service providers shall without delay report to the authority operating as the financial intelligence unit all data, facts and circumstances that indicate that the person subject to the financial restrictive measures and the freezing of assets has funds or economic resources in the territory of the Republic of Hungary that are subject to financial restrictive measures or the freezing of assets

During the implementation of this Act it is expedient for the service provider to apply the rules of the MLA on reporting obligations, on the prohibition of disclosure, on the screening system, on record-keeping and on document retention and to incorporate the knowledge related to this Act into the training and extension training of employees.

The procedure to be applied for persons and organisations included on the lists related to restrictive measures ordered by the European Union must be demarcated from the measures carried out for persons and organisations included on the lists prepared by the UNO and by the USA.

Financial service providers shall employ the provisions of Act CLXXX of 2007 for the lists of the Union, which also incorporate the lists specified by the annexes of the council regulations (Council Regulations 881/2002/EC and 2580/2001/EC) to be directly implemented and created with regard to the fight against terrorist financing and with regard to the persons and organisations included on those lists.

If in order to combat terrorist financing a financial service provider also screens against other lists, including other lists issued by the Union, then for persons and organisations included on such lists the financial service provider shall conduct reporting pursuant to Paragraph (1) of Article 23 of the MLA, i.e., if some data, facts or circumstances emerge that indicate terrorist financing, provided that the data is not identical to persons or organisations included on lists specified in the annexes to the Council Regulations created in order to combat terrorist financing and which are to be applied directly.

## **2.22. Prohibition of disclosure**

Pursuant to the MLA and to the international standards the financial service provider may not inform the customer or any third person or organisation of the fact that a report has been made or that information has been provided in response to a request or of the contents of such information, or that the execution of a transaction has been suspended, or of the identity of the reporting person, or of whether or not a criminal investigation has been initiated against the customer.

The service provider shall ensure that the act of reporting, the contents of the report and the identity of the reporting person shall remain secret. Both domestic and international regulations treat reporting as confidential information that should be protected more strictly than data included within the scope of banking secrets. The legislator provides a rather tight taxative list within the Act for the cases where an exception from the prohibition of disclosure is possible.

The prohibition of disclosure does not extend to disclosure to supervisory organisations and to investigative authorities conducting a criminal procedure if they request information in order to fulfil their responsibilities as specified in legal statutes.

This prohibition shall not apply to data forwarded for consolidated supervision or for supplementary supervision of financial conglomerates as specified under the laws governing the industry sectors, to the disclosure of information between institutions of member states or third countries which impose requirements equivalent to those laid down in this Act and which are subject to supervision with regard to compliance with these requirements.

For service providers providing financial services, supplementary financial services, investment services, supplementary services for investment services, insurance services, insurance brokerage and employer's pension services, services related to the commodities exchange, postal currency brokerage, postal money transfers, the receipt and delivery of domestic and international postal money orders or operating as a voluntary mutual insurance fund the prohibition shall not apply to the disclosure of information between two or more involved service providers, subject to the following conditions:

- The information should relate to the same customer and to the same transaction;
- Of the two or more financial service providers at least one should be engaged in activities governed by the MLA and the other service providers should be domiciled in another member state or in a third country that imposes requirements equivalent to those laid down in this Act;
- The involved service providers should be engaged in identical activities as specified under Paragraph (1) of Article 1 of the MLA;
- The service providers should be subject to requirements equivalent to the domestic requirements with regard to professional secrecy and the protection of personal data.

### **2.23. Training**

Financial Service Providers shall take appropriate measures to acquaint their employees, engaged in activities pursuant to Paragraph (1) of Article 1 of the MLA, with the legislative provisions related to money laundering and terrorist financing, to recognise transaction orders that enable or implement money laundering or terrorist financing and to be able to proceed in compliance with this Act if some data, facts or circumstances emerge that indicate money laundering or terrorist financing. For this purpose the designated person shall develop rules for training and extension training wherein appropriate measures shall be taken to train

new employees and to organise regular extension training for employees at least once every year, to record and document such training and to assess the knowledge acquired.

In addition to the regulations on money laundering the training curriculum should also include the rules for money laundering and terrorist financing as contained in the money laundering statutes, in the MLA and in the Penal Code, as well as the international materials related to money laundering.

The HFSA proposes that service providers use examinations to control training and that they retain the results of such examinations and amend the training curricula based on the experience obtained. The occurrence of training and examinations must be documented. It is expedient for the designated person to develop the rules for training and extension training.

**The following represent the legal framework for the fight against money laundering:**

- 1.) Act LXXXIII of 2001 on the fight against terrorism, on tightening the provisions for the prevention of money laundering and on the implementation of certain restrictive measures;
- 2.) Act IV of 1978 on the penal code;
- 3.) Act CXXXVI of 2007 on the prevention and deterrence of money laundering;
- 4.) Act XCII of 1996 on credit institutions and financial enterprises;
- 5.) Act CXX of 2001 on the capital market;
- 6.) Act LX of 2003 on insurance institutions and insurance activities;
- 7.) Act CXXXVIII of 2007 on investment enterprises and service providers related to the commodities exchange and on the rules for their permitted activities;
- 8.) Act XCVI of 1993 on voluntary mutual insurance funds;
- 9.) Government Decree No. 227 of 2006 (of November 20) on funds transfer services and electronic payment instruments;
- 10.) Regulation No. 21 of 2006 (of November 24) issued by the National Bank of Hungary on the performance of payments;
- 11.) Resolution No. 24 of 1998 issued by the Constitutional Court;
- 12.) The Vienna Convention of 1988 Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, enacted with Act L of 1998 (Article 5);
- 13.) Act CI of 2000 on the enactment of the Strasbourg Convention of 1990 (on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime)
- 14.) EU Directive No. 91/308 for the prevention and deterrence of money laundering;
- 15.) EU Directive No. 2001/97 for the prevention and deterrence of money laundering;
- 16.) Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing;
- 17.) Council Directive 2006/70/EC of 1 August 2006 on the specification of implementation measures for Directive 2005/60/EC of the European Parliament and of the Council, with regard to the concept of “politically exposed persons” and to the technical requirements for simplified customer due diligence measures and for exemptions provided on the basis of financial activities conducted on an ad-hoc or highly restricted basis;
- 18.) The Customer Due Diligence Recommendation of the Basel Committee for Banking Supervision and the similar recommendations of the IOSCO and of the IAIS;
- 19.) The 40+9 Recommendations of the FATF.