

# [EBF Anti Money Laundering Report]

[2009]

[Brussels, 2009]

## **Credits**

### ***Editor Responsible***

Guido Ravoet

Secretary General

### ***Coordination***

Séverine Anciberro

Adviser

Retail Financial Services, Legal and  
Social Affairs

[s.anciberro@ebf-fbe.eu](mailto:s.anciberro@ebf-fbe.eu)

### ***Layout & Design***

Laura Cerrato

Please quote when making reference to this report.

## [Table of Contents]

<b>[Table of Contents]</b> .....	<b>1</b>
<b>[Introduction]</b> .....	<b>2</b>
<b>[Data per Country]</b> .....	<b>3</b>

AUSTRIA.....	3
BELGIUM .....	8
BULGARIA .....	11
CZECH REPUBLIC .....	21
DENMARK .....	34
ESTONIA.....	39
FRANCE.....	49
GERMANY .....	57
GREECE .....	62
HUNGARY .....	78
IRELAND.....	83
ITALY .....	89
LATVIA.....	109
LIECHTENSTEIN .....	120
LUXEMBOURG.....	131
MALTA .....	143
THE NETHERLANDS .....	151
NORWAY .....	162
POLAND.....	169
PORTUGAL.....	174
SLOVAK REPUBLIC.....	179
SLOVENIA .....	189
SPAIN.....	199
SWEDEN.....	206
SWITZERLAND.....	211
UNITED KINGDOM.....	218

## [Introduction]

This report has been drafted by the Anti-Money Laundering and Anti-Fraud Committee of the European Banking Federation (EBF) based on contributions submitted by national banking associations.

This extensive document offers an inventory of national regulations on money laundering in more than 25 countries in Europe with a focus on the implementation of Directive 2005/60/EC<sup>1</sup> of the European Parliament and of the Council of 26 October 2005 on the Prevention of the use of the Financial System (the” Third EU Anti-Money Laundering Directive”).

National legislation are detailed and listed with identical headings (type of legislation, business covered, reporting procedures, identification requirements, etc.) which introduce some valuable elements of comparison among countries.

Please note that the Report is based on information collected from August 2008 to March 2009. The EBF cannot be held responsible or liable in any way for possible omissions or inaccuracies.

EBF Legal Department  
European Banking Federation (EBF)  
Brussels

---

<sup>1</sup> 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, Official Journal of the European Union, 25.11.2005, L 309/15

## [Data per Country]

### AUSTRIA

The Austrian Bankers' Association

#### [ANTI-MONEY LAUNDERING /CTF LEGISLATION]

Austria criminalized money laundering in 1993.

To implement the EU's Third Money Laundering Directive (Directive 2005/60/EC), an amendment to the Banking Act has been in effect since January 1, 2008.

The preventive measures obliging the financial sector can be found in the respective sectoral Acts (banking, insurance – insurance intermediaries fall under the Trade Act [Gewerbeordnung GewO] – securities and stock exchange). CDD measures have generally been in force since the implementation of Directive 91/308/EEC (“1st EU AML Directive”), were adapted under Directive 2001/97/EC (“2nd EU AML Directive”) and have recently been refined in line with Directive 2005/60/EC (here after “3rd EU AML Directive”). The last amendments to the Securities Supervision Act (WAG) implementing the 3rd EU AML Directive became effective on December 15, 2007, amendments to the Banking Act and the VAG on January 1, 2008 and amendments to the Trade Act on February 27, 2008. AML/CFT measures apply to all institutions covered by these acts, with the exception of insurance companies and intermediaries outside the underwriting and placement of life insurance and other investment related insurance, i.e. no financial institution under the FATF definition has been exempted. Money remittance businesses require a banking license from the FMA and are subject to supervision.

On January 1, 2008, responsibility for on-site inspections of banks, exchange businesses and money transmitters moved from the Financial Market Authority (FMA) to the Austrian National Bank. These on-site inspections, including inspections at subsidiaries abroad, are all-inclusive, and will require analysis of financial flows and compliance with money laundering regulations.

Amendments to the Customs Procedures Act and the Tax Crimes Act of 2004 and 2006 address the problem of cash couriers and international transportation of currency and monetary instruments from illicit sources.

Since 1996, legislation has provided for asset seizure and the forfeiture of illegal proceeds. The Austrian Criminal Code provides for the criminalization of money laundering and terrorist financing. Regulations in the Code of Criminal Procedure: In connection with money laundering, organized crime and terrorist financing, all assets are subject to seizure and forfeiture, including bank assets, other financial assets, cars, legitimate businesses, and real estate. Courts may freeze assets in the early stages of an investigation.

## [PENALTIES IN NATIONAL LAW FOR FAILURE TO RESPECT OF THE NATIONAL PROVISIONS TO THE DIRECTIVE]

Concerning financial institutions administrative offences are to be punished by the FMA (Financial Market Authority) unless the act constitutes a criminal offence falling into the jurisdiction of the courts.

## [CENTRAL AUTHORITY FOR REPORTING]

Austria's financial intelligence unit (FIU) is located within the Austrian Interior Ministry's *Bundeskriminalamt* (Federal Criminal Intelligence Service). The FIU is the central repository of suspicious transaction reports (STRs) and has police powers.

## [PERSONS RESPONSIBLE FOR REPORTING]

In cases where a credit institution or financial institution suspects or has reasonable grounds to suspect then credit institutions and financial institutions must report such suspicions to the relevant authority (Article 6 Security Police Act [*Sicherheitspolizeigesetz – SPG*]).

## [BUSINESS COVERED BY THE LEGISLATION (WHICH SPECIFIC PERSONS: NOTARIES, LAWYERS...)]

In Austria, the preventive measures obliging DNFBPs (Designated Non-Financial Businesses and Profession) can be found in the different Acts governing the respective businesses and professions. CDD measures have generally been in force since the implementation of Directive 2001/97/EC (“2nd EU AML Directive”) adapting Directive 91/308/EEC (“1st EU AML Directive”) and have recently been extended to further DNFBPs (TCSPs, traders in all kinds of goods, insurance intermediaries) as well as refined in line with Directive 2005/60/EC (“3rd EU AML Directive”). The last amendments to the Lawyer's Act (*Rechtsanwaltsordnung – RAO*) and Notarial Code (*Notariatsordnung – NO*) implementing the 3rd EU AML Directive became effective on December 29, 2007, amendments to the Trade Act (*Gewerbeordnung – GewO*) on February 2, 2008 and to the Chartered Public Accountants and Tax Consultants Practice Directive (*Wirtschaftstreuhandberufs-Ausübungsrichtlinie – WT-ARL*) and the Directive concerning the Practice of the Accountancy Professions (*Bilanzbuchhaltungs-(Berufs)Ausübungsrichtlinie – BiBu-ARL*) on April 23, 2008 and May 1, 2008.

A proposal implementing the 3rd EU AML Directive in the Law on games of chance (*Glücksspielgesetz – GSpG*) came into force on August 27, 2008 (Federal Law Gazette I No 126/2008).

The Chartered Public Accountants and Tax Consultants Practice Directive (*Wirtschaftstreuhandberufs-Ausübungsrichtlinie – WT-ARL*) and the Directive concerning the Practice of the Accountancy Professions (*Bilanzbuchhaltungs-(Berufs)Ausübungsrichtlinie –BiBu-ARL*) are based on Art. 83 §. 2 of the Act on the Profession of Chartered Public Accountants and Tax Consultants (*Wirtschaftstreuhandberufsgesetz – WTBG*) and Art. 69 §. 2 Balance Sheet Accounting Act (*Bilanzbuchhaltungsgesetz – BiBuG*) respectively and approved by the MoE. These Directives are regulations in the meaning of the Federal Constitutional Law (*Bundes-Verfassungsgesetz – B-VG*). Insurance intermediaries are also regulated in the Trade Act (*GewO*).

## [PREDICATE OFFENCES COVERED]

Austria has adopted a combined approach, listing all felonies and a number of misdemeanours in § 165 StGB (Penal Code) as predicate offences for money laundering. Felonies are intentional offences sanctioned with life imprisonment or imprisonment of more than three years whereby the maximum sanction is the determining factor for the differentiation between felonies or misdemeanours. Regulations are stricter for money laundering by criminal organizations and terrorist “groupings,” because in such cases the law requires no proof that the money stems directly or indirectly from prior offenses.

## [IDENTIFICATION]

The Banking Act of 1994 creates customer identification, record keeping, and staff training obligations for the financial sector. Entities subject to the Banking Act include banks, leasing and exchange businesses, safe custody services, and portfolio advisers. The law requires financial institutions to identify all customers when beginning an ongoing business relationship. In addition, the Banking Act requires customer identification for all transactions of more than 15,000 € for customers without a permanent business relationship with the bank. Identification procedures require that all customers appear in person and present an official photo identification card. These procedures also apply to trustees of accounts, who must disclose the identity of the account beneficiary. Procedures allow customers to carry out non face-to-face transactions, including Internet banking, on the basis of a secure electronic signature or a copy of a picture ID and a legal business declaration submitted by registered mail.

To implement the EU’s Third Money Laundering Directive (Directive 2005/60/EC), an amendment to the Banking Act has been in effect since January 1, 2008. The new regulations tighten customer identification procedures by requiring renewed identification in case of doubt about previously obtained ID documents or data as well as requiring personal appearances of trustees. Regulations also require institutions to determine the identity of beneficial owners and introduce risk-based customer analysis for all customers. Financial institutions must also begin to implement these requirements in their subsidiaries abroad. The 2008 Banking Act amendment also broadens the reporting requirement by replacing “well-founded suspicion” with “suspicion

or probable reason to assume” that a transaction serves the purpose of money laundering or terrorist financing or that a customer has violated his duty to disclose trustee relationships.

The Securities Supervision Act of 1996, which covers trade of securities, shares, money market instruments, options, and other instruments listed on an Austrian stock exchange or any regulated market in the EU, refers to the Banking Act’s identification regulations. The Insurance Act of 1997 includes similar regulations for insurance companies underwriting life policies. An amendment to the Insurance Act of 1997, in effect since January 1, 2008, tightened record keeping requirements for insurance companies.

## Enhanced due diligence obligations

In situations which by their nature can present a higher risk of money laundering or terrorist financing, credit institutions and financial institutions must apply additional due diligence measures in addition to the obligations pursuant to Article 40 §. 1, 2, 2a and 2e Banking Act on a risk-sensitive basis. In any event these measures apply if the customer has not been physically present for identification purposes (for example, non face-to-face transactions, Internet banking), with regard to cross-border correspondent banking relationships and with regard to transactions or business relationships to politically exposed persons from other Member States or from third countries:

- a) credit institutions and financial institutions must have appropriate risk-based procedures to determine whether the customer is a politically exposed person;
- b) credit institutions and financial institutions must obtain senior management approval before establishing business relationships with such customers;
- c) credit institutions and financial institutions must take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction; and
- d) credit institutions and financial institutions must conduct enhanced ongoing monitoring of the business relationship.

In cases where a financial institution is unable to establish customer identity or obtain other required information on the business relationship, it must decline to enter into a business relationship or process a transaction, or terminate the business relationship. The institution must also consider reporting the case to the FIU. The law also requires financial institutions to keep records on customers and account owners.

## [EXISTING GUIDELINES TO THE BANKING INDUSTRY]

On its website, the Financial Market Authority (FMA) has published several circular letters with details on customer identification, money laundering and terrorist financing regulations, and reporting of suspicious transactions.

## [GENERAL FEEDBACK (NEW MODUS OPERANDI, TRENDS, REAL CASES, etc)]

The FIU provides a general feedback by publishing an annual report.

## [PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK STAFF IN THE EVENT OF NOTIFICATION) OF THE INSTITUTIONS OR PERSONS COVERED BY THIS DIRECTIVE ]

The Banking Act includes a due diligence obligation, and the law holds individual bankers responsible if their institutions launder money. The Banking Act and other laws provide “safe harbor” to obligated reporting individuals, including bankers, auctioneers, real estate agents, lawyers, and notaries. The law excuses those who report from liability for damage claims resulting from delays in completing suspicious transactions.

## [CONSERVATION OF RECORDS AND DOCUMENTS]

The law also requires financial institutions to keep records on customers and account owners: Credit institutions and financial institutions must retain the following: documents serving the purpose of identification pursuant to for at least five years after the termination of the business relationship with that customer; documentation and records of all transactions for a period of at least five years after their execution.

## [STEPS TAKEN TO INCREASE AWARENESS OF THE PHENOMENON OF MONEY LAUNDERING (E.G.: TRAINING, INFORMATION...)]

The Banking Act requires that banks take suitable measures to familiarise the staff responsible for the execution of transactions with the provisions intended to prevent or suppress money laundering or terrorist financing; these measures must also include the participation of the responsible employees in special training programmes in order to train the employees to recognise transactions which may be connected to money laundering or terrorist financing and to behave correctly in such cases. Regular dialogues are organized by FMA and the banking industry on practical issues. The Association keeps its members informed about legislative developments and other trends. Banks organise their own training programmes.

## BELGIUM

Febelfin

### [ANTI-MONEY LAUNDERING /CTF LEGISLATION]

Since the beginning of 2007, Belgium has been preparing a draft text for the transposition of the 3rd Directive. Due to the political problems Belgium struggled with in 2007 and 2008, this bill has never been submitted to Parliament. At the beginning of 2008, a new version was presented which takes into account the two arrests of the Constitutional Court about the lawyers' obligations in the field of the fight against money laundering. This text also serves as a response to the 2008 FATF assessment report, which points out a number of issues for which the existing provisions should be improved. Currently, the text of the draft law is being analysed by the Council of State and its voting in Parliament and publication in the *Moniteur belge* is scheduled for the summer of 2009.

Several of the new requirements imposed by the FATF standards (i.e. the June 2003 40 new recommendations and the 9 special recommendations as for the fight against the financing of terrorism) and hence by the new Directive, have already been integrated into Belgian law by the Law of January 12, 2004 modifying the Law of January 11, 1993 on preventing the financial system from being used for the purpose of money laundering. Consequently, there is no need to adapt the Belgian law governing the fight against the financing of terrorism and the detailed list of criminal activities that yield money to be laundered. The current list of criminal activities mentioned in article 3 of the Law of January 11, 1993 indeed is broad enough to cover all of the offences which, under Belgian law, lead to imprisonment for at least six months. Nevertheless, the text of Directive 2005/60/EC imposes a number of very strict conditions which make it necessary to further adapt the Belgian regulations.

### [BUSINESS COVERED BY THE LEGISLATION (WHICH SPECIFIC PERSONS: NOTARIES, LAWYERS...)]

#### **Modifications aimed at taking into account the professional secrecy of lawyers, notaries, company auditors, expert accountants and tax counsellors**

In its January 23, 2008 arrest, the Constitutional Court has given its interpretation of the obligations imposed on lawyers in the field of information and collaboration : the obligation as for the professional secrecy governing legal counseling, is still valid, except when the legal counselor is involved in money laundering or financing of terrorism, provides legal counsel for the purpose of money laundering or financing of terrorism or is well aware of the fact that his client calls on him with those aims in mind. In those cases, the obligation to make a declaration is legitimate.

In the wake of this arrest of the Constitutional Court, it has been decided by law that the notaries, company auditors, expert accountants, tax counsellors, registered accountants as well as tax accountants mentioned in article 2bis of the Law of January 11, 1993 are also exempt from the obligation to make a declaration, when they provide legal counselling.

The new measures that have been introduced under Directive 2005/60/EC as for due diligence towards customers, take into account the specific character of a lawyer's profession. This explains why the law provides that a lawyer does not have to put an end to the relationship between him and his client, only because he did not succeed in fully identifying the latter, for the purpose of preventing the defendant's rights from being weakened.

Finally, the draft law states that, as for the professions that are subject to professional secrecy as mentioned in article 458 of the Code of criminal law, the possibility of an employee making a declaration should be excluded. In that case, it will be necessary to call upon the person actually in charge or the professional to make a declaration.

### **Making some of the obligations applicable to non-financial professions**

This extension deals with the editing of a written report, when a transaction or fact is deemed to be unusual and with putting into practice internal supervision procedures in order to be able to detect transactions and facts which one suspects to be linked to money laundering of financing of terrorism.

#### [IDENTIFICATION]

The Directive contains an exact definition of the actual beneficiary which should be transposed into Belgian law for the purpose of including objective criteria that can help the institutions and professions mentioned in the law in determining the natural persons who are deemed being in control of an artificial person of a legal entity.

For the purpose of enhanced legal certainty, a provision dealing with the stricter measures for vigilance towards politically exposed persons has been introduced into the draft, the requirements laid down in the Directive as well as the results of the FATF assessment for Belgium being taking into account though.

Several measures aim at improving the provisions governing the identification of the customer and the actual beneficiary. As a result, the derogations vis-à-vis the obligatory identification as laid down in the current article 6 of the Law of January 11, 1993, will not apply when there is a suspicion as to money laundering or financing of terrorism. If the measures for the identification of the actual beneficiary do not yield any result, the business relationship must be ended. However, one agrees upon the fact that checking the data for identifying the actual beneficiary is a commitment as to the means and no commitment as to the result.

An important modification concerns the identification, as actual beneficiaries, of major shareholders of companies among the customers.

The draft law contains two measures which seem to be necessary in order to enable the persons and institutions to which the law applies, to meet their obligation to identify the actual beneficiaries of the companies that are customers. According to the draft law, those companies must provide the persons and institutions subject to the law, with the information required about their shareholders who reach or surpass the limit mentioned above. In order to make it possible for companies which have issued bearer shares or dematerialised shares, to meet this obligation to inform the persons and institutions of which they are or will become customers, the draft law makes sure they actually have the information needed at their disposal.

## [PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK STAFF IN THE EVENT OF NOTIFICATION) OF THE INSTITUTIONS OR PERSONS COVERED BY THIS DIRECTIVE ]

Protecting those who make a declaration, has been a major concern of the financial sector for several years.

Febelfin has made an urgent call for a transposition into Belgian law of the principles laid down in article 27 of the Directive.

Consequently, the draft law for the transposition of the Directive provides that *«the competent authorities take any measure that is adequate for protecting the employees working for the companies or persons subject to this law, against any kind of threat or hostile act, when these employees inform their company or the Financial Information Processing Unit of their suspicion about money laundering or financing of terrorism»*.

However, currently there is not really such thing as an adequate protection of employees and this should be taken into account.

One of the problems is the situation in which the employees are confronted with the suspect and another is that of disclosing the identity of employees who have informed the Financial Information Processing Unit mentioned in articles 20 or 23 to 27 of the law.

This problem has been brought to the attention of the FIPU, which has edited a circular. This circular has been sent electronically to all members of the coordination group of the Expert Network dealing with economic, financial and tax crime, and a copy of it has been enclosed. In March 2008, this text also has been sent to all public prosecutor's departments for information and the attention of the latter has been drawn on the problem of sensibilising the local police force.

At the beginning of 2009, the public prosecutor at a court of appeal sent a letter to all public prosecutor's departments in order to point out the importance of forwarding this document, should it be that some police services have not been informed.

### [ANTI-MONEY LAUNDERING /CTF LEGISLATION]

- The Law on Measures against Money Laundering/AML Act;
- The Rules for the implementation of the AML Act;
- The Law on Measures against Financing of Terrorism.

### [PENALTIES IN NATIONAL LAW FOR FAILURE TO RESPECT THE NATIONAL PROVISIONS OF THE DIRECTIVE]

There are administrative sanctions for breaching the different provisions of the Law on Measures against Money Laundering implemented by the Directive. The administrative sanctions for a committed breach of the AML Act is a fine - in the case of a sole trader or a legal person - a proprietary sanction that varies from 500 to 50 000 BGN.

### [CENTRAL AUTHORITY FOR REPORTING]

The Central authority for reporting is the Directorate "Financial intelligence" of State Agency "National Security".

### [PERSONS RESPONSIBLE FOR REPORTING]

These are, as follows:

1. The Bulgarian National Bank, credit institutions, carrying out activity on the territory of the Republic of Bulgaria, financial houses, the exchange offices and the companies carrying out materialized money transfers;
2. Insurers, re-insurers and insurance intermediaries with a seat in the Republic of Bulgaria; insurers, re-insurers and insurance intermediaries from a Member State of the European Union, or from a State - party to the Agreement on the European Economic Space - who perform activity on the territory of the Republic of Bulgaria; insurers with a seat in states, different from the enlisted, and which received licence from the Commission for financial supervision to perform activity in the Republic of Bulgaria through a branch, insurance intermediaries with a seat in countries, different from the indicated, entered into the register of the Financial Supervision Commission;
3. Collective investment schemes, investment brokers and managing companies;
4. Pension insurance companies and health insurance companies;

5. Bodies for privatisation;
6. Persons organising assignment of public orders;
7. Persons organising and conducting gambling games;
8. Corporate bodies where there are mutual support savings;
9. Persons conceding money loan against pawning of chattels;
10. Post services accepting or receiving money or other valuables;
11. Notaries;
12. Market operator and/or regulated market;
13. Leasing enterprises;
14. State and municipal bodies concluding concession contracts;
15. Political parties;
16. Trade unions and professional organisations;
17. Corporate non-profit bodies;
18. Certified expert accountants and specialised auditing enterprises;
19. The bodies of the National Revenue Agency;
20. Customs bodies;
21. Entrepreneurs selling automobiles by profession when the payment implemented in cash and the value is over 30 000 BGL or the equivalent in foreign currency;
22. Sport organisations;
23. The central Depository;
24. Persons who, by profession, carry out transactions with goods, in case of cash payment and its value amounts to over 30 000 BGN or the equivalent in foreign currency;
25. Traders of weapons, petrol, and petrol products;
26. Persons, who as a profession, implement consultations in the field of tax levying;
27. Wholesale traders;
28. Persons, who as a profession implement legal consultations, when:
  - a) they participate in the planning or the fulfilment of operation or transaction of their client for:
    - aa) purchase and sale of immovable property or transfer of enterprise to trader;
    - bb) management of money, securities or other financial assets;
    - cc) opening or disposing with bank account or account for securities;
    - dd) providing resources for establishing of trader, increase of the capital of a commercial company, conceding of loan or any other form of providing resources for accomplishing the activity of the trader;

- ee) establishing, organising the activity or management of a trader or of another legal person, offshore company conceded to fiduciary management or other similar structure;
  - ff) trust management of property;
  - b) act for the account or in the name of their client in whatever financial operation or transaction with immovable property;
29. Persons, who implement by profession, mediation in transactions with immovable properties.
30. Persons, who by profession provide:
- a. address of management, mailing address or an office for registration purposes of a legal person;
  - b. service related to registration of a legal person, offshore company, trust management company or any other similar structure;
  - c. services of trust management of property or of a person under item "b";
31. The persons in item 28 shall not be obliged to advise per the procedure of this law, the information - made available to them, in or with regard to participation in court or pre-court proceedings - that is pending, to be initiated or has been closed, including information, related to determination of the legal status of a client.

[BUSINESS COVERED BY THE LEGISLATION (WHICH SPECIFIC PERSONS: NOTARIES, LAWYERS...)]

See above.

The business covered includes notaries, lawyers, etc.

[PREDICATE OFFENCES COVERED]

According to the AML Act money laundering in the sense of this law shall be:

1. transformation or transfer of possessions acquired through criminal activities or from an act of participation in such activity, in order to hide or cover the illegal origin of the possessions or in order to assist a person, participating in perpetration of such activity in order to avoid legal consequences of his/her act;
2. hiding or covering of the essence, of the source, the location, the disposition, the movement or the rights with regard to the possession, acquired through a crime or an act of participation in such activity;

3. acquisition, possession, keeping or use of possessions with the knowledge at the moment of receiving that they have been acquired through a crime, or from an act of participation in such activity;
4. participation in any of the actions under item 1 – 3, association with the purpose of perpetration of such an act, trial to perpetrate such an act, as well as assisting, instigation, facilitation of perpetration of such an activity or its covering;

Money laundering shall be considered also when the activity, through which the possessions under the above texts have been acquired, has been carried out in a Member State of the European Union or in another country and does not come under the jurisdiction of the Republic of Bulgaria.

As a summary, according to the Bulgaria legislation, predicate offence covered is every criminal activity through which one can acquire (get any) property.

## [IDENTIFICATION]

### **a. Definition (e.g.: PEPs, beneficial owner, thresholds...)**

According to the Rules on the Implementation of the Law on Measures against Money Laundering:

**PEPS** are potential customers, existing customers, and beneficial owners of the client that is a legal person, who are:

1. heads of State, heads of government, ministers and deputy or assistant ministers;
2. members of parliament;
3. members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
4. members of courts of auditors;
5. members of the boards of central banks;
6. ambassadors and chargés d'affaires;
7. high ranking officers in the armed forces;
8. members of the administrative, management or supervisory bodies of State-owned enterprises;

The categories stipulated in items 1-7 include, where applicable, the respective positions in the institutions and bodies of the European Union and of the international organizations.

The measures stipulated for the categories of customers in items 1-8 shall also be applied in respect of mayors and deputy mayors of counties, the mayors and chairpersons of the districts and the chairpersons of the municipal councils.

The categories stated in items 1-8 do not include officials at intermediate or more junior level.

For the purpose of the AML act, the related person shall include:

1. spouse or persons who live in factual partnership with them;
2. relatives of descending line to the first degree of affinity and their spouse or persons who live in factual partnership with them;
3. relatives of ascending order of the first degree of affinity;
4. any natural person who is known or can be supposed, from publicly available information, to have joint beneficial ownership of a legal person or any other close business relations with a person referred to in items 1-8 above;
5. any natural person who has sole beneficial ownership of a legal person which is known or can be supposed from publicly available information to have been set up for the benefit de facto of the person referred to in items 1-8 above.

**b. Beneficial owner of a customer-legal entity is:**

1. natural person or natural persons who directly or indirectly own more than 25% of the shares or of the capital of a customer-legal entity, or of another similar structure, or exercise direct or indirect control over it;
2. natural person or natural persons in favour of which more than 25% of the property is controlled or distributed, whenever the customer is a foundation, a non-profit organisation or another person performing trustee management of property or property distribution in favour of third persons;
3. a group of natural persons in favour of whom a foundation, or a public benefit organisation, or a person performing trustee management of property or property distribution in favour of third persons is established, or acts, when these persons are not directly determined but can be determined by specific signs.

**b. Identification threshold amount**

According to the AML Act, the persons responsible for reporting shall be obliged to identify their clients at establishing trade or in professional relations, including when opening a bank account as well as when implementing an operation or concluding a transaction for an amount exceeding 30 000 BGN or the equivalent in foreign currency, and the persons of items 1 – 4, 9 – 11, 13 and 28 from the above point: “Persons Responsible for Reporting” also at implementing an operation or at concluding transaction in cash with value exceeding 10 000 BGN or the equivalent in foreign currency.

The stated threshold of 30 000 BGN is considered to be reached if the transactions or operations carried out do not separately exceed threshold or the equivalent of this amount in foreign currency. From the circumstances of their performance it can be supposed that these operations or transactions are related.

**c. Identification at a distance (non face to face)**

In the case of establishment of commercial or professional relations, or implementation of operation or transaction through electronic statement, electronic document or electronic signature - or any other form - without the presence of the client, the persons responsible for reporting shall be obliged to undertake appropriate measures for certifying the authenticity of the identifying data of the client.

Such measures can be:

- verification of the presented documents;
- requirement of additional documents;
- confirmation of the identification by another person responsible for reporting or by a person obliged to apply measures against money laundering in a Member State of the European Union, or;
- establishing the requirement that the first payment of the operation or the transaction to be implemented through an account opened in the name of the client in a Bulgarian bank or in a branch of foreign bank, receives permission (licence) by the Bulgarian National Bank to implement activity in the country through a branch or in a bank from a Member State of the European Union.

**d. Outsourcing of identification to third parties**

According to the Bulgarian legislation, the Bulgarian National Bank, the credit institutions referred to in item 1 from the above point: *Persons Responsible for Reporting*, as well as the persons in items 2, 3 and 4, may refer to preceding client identification, carried out by a credit institution under the following conditions:

1. the seat of business of the credit institution that has carried out identification, is in the Republic of Bulgaria, in another Member State, or in a country corresponding to the law list;
2. the information required pursuant to the means of identification shall be available to the person, referring to preceding identification, carried out by a credit institution;
3. upon request by the credit institution, which has carried out preceding identification, the person is able to provide immediately identification with certified copies of the documents of the identification, referring to the person.

The reference of the identification under the above shall not exempt the person from liability for non-fulfilment of the requirements for the identification as per the means of identification.

**e. Means of identification**

Pursuant to the Bulgarian AML legislation, the identification of the clients and verification of their identification shall be implemented:

1. for corporate bodies; presenting an official excerpt for the current status of the corresponding register, and if the person is not subject to registration; a certified copy of the establishing act, and registration of the name, the headquarters, the address and the representative;
2. for individuals; presenting an official identification document and registration of its kind, issuer, as well as the name; address, and unified civil number; and for individuals with the quality of sole entrepreneur, also presenting the documents of item 1.

The persons responsible for reporting shall identify natural persons who are the real owners of a client, i.e. legal person, as well as undertake actions for verification of their identification depending on the type of client and level of risk, resulting from determination of customer relations and/or implementation of transactions or operations with such clients. Provided that there is not any other opportunity, identification can be carried out through a declaration, signed by the legal representative or the proxy of the legal person. The conditions and the procedure - for releasing from the obligation for identification, as well as the form and procedure for releasing from the obligation for identification, and the form and procedure for submission of the declaration - shall be set out in the regulations implementing the Law.

In the cases where a certain activity is subject to licensing, permit or registration, the persons carrying out transactions and operations in connection with this activity shall present a copy of the respective licence, permit or registration certificate.

**f. Source of information (e.g.: public register for the identification of beneficial owner)**

The main source of information is the respective register.

The persons responsible for reporting verify the information for the identification by means of one or more of the following methods:

1. revision of the balance sheet, the financial reports and the accountability bills (including the auditing report, if any);
2. inquiry, through an intermediary, about business information;
3. inquiry assignment to lawyers' partnerships or either natural or legal persons rendering accountancy services of good reputation;
4. demanding bank references;
5. demanding references from persons who are, or have been commanding the services of the customer, or either have been or are in commercial or professional relations with them;
6. obtaining information from the commercial register or other sources to find out whether the company has been or is in procedure for insolvency, obliteration, liquidation or termination;
7. making use of other independent sources (accessible databases of public and private organisations, internet);
8. visits to production premises or administrative offices of the company;
9. telephone, postal or e-mail contacts.

## [PRODUCTS AND TRANSACTIONS CHARACTERISED BY A HIGH/LOW RISK OF MONEY LAUNDERING]

Products and transactions which might lead to anonymity are covered by the law of high risk. In this regard, the persons responsible for reporting are obliged to apply the following measures:

1. analyze the risk associated with the respective product or transaction while taking into consideration factors such as the use of the product in more than one jurisdiction, the size of the financial resources associated with the products, and transactions and the profile of the customers of the respective product or transaction;
2. undertake constant monitoring of the respective product or transaction and take appropriate measures to determine the level of risk;
3. acquaint the employees with the risk related to the respective product or transaction and the measures necessary to counteract the risk;

4. document the risk-analysis undertaken and the measures taken to counteract the risk.

## [EXISTING GUIDELINES TO THE BANKING INDUSTRY]

No guidelines for the banking industry are available in Bulgaria. This situation causes the banks, difficulties in the implementation of the AML rules, which, in cases such as identifying and applying the respective measures to the PEPS are significant (in addition the Bulgarian definition is very broad and includes national PEPS and the persons related to them).

## [GENERAL FEEDBACK (NEW *MODUS OPERANDI*, TRENDS, REAL CASES, etc.)]

No general feedback is foreseen in the legislation.

According to the law,, Directorate "Financial intelligence" of State Agency "National Security" shall provide, to the reporting person, information related to the implemented by his/her notification. The decision with regard to the scope of information, supposed to be provided as a feedback for each specific case of notification, shall be taken by the Director of the Agency.

## [PURPOSES FOR WHICH THE FEEDBACK INFORMATION MAY BE USED]

The feedback for a specific case of notification may be used in the decision-making process on whether or not to terminate the relationship with the client.

## [PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK STAFF IN THE EVENT OF NOTIFICATION) OF THE INSTITUTIONS OR PERSONS COVERED BY THIS DIRECTIVE ]

The Law on Measures against Money Laundering provides the following:

- For suspicion of money laundering, the persons responsible for reporting shall be obliged to immediately notify Directorate "Financial intelligence" of State Agency "National Security" before the implementation of the operation or the transaction, delaying its fulfilment within the admissible term according to the normative acts damaging the respective type of activity.
- The notification of the Directorate can also be carried out by employees of the persons responsible for reporting who are not in charge of the implementation of the measures against money laundering. The Directorate shall preserve the anonymity of these employees.

- In the case of revealing information in compliance with AML Act, no responsibility shall arise, if afterwards it is determined that no crime has been committed, and that the operations and the transactions have been lawful.

## [CONSERVATION OF RECORDS AND DOCUMENTS]

The persons responsible for reporting, shall be obliged to conserve the data about the clients and the documents about the implemented transactions and operations, for a period of 5 years. For the clients, the term starts from the beginning of the calendar year

The data and the documents shall be conceded to Directorate "Financial intelligence" of State Agency "National Security", upon request, in the original or officially certified copy.

## [STEPS TAKEN TO INCREASE AWARENESS OF THE PHENOMENON OF MONEY LAUNDERING (E.G.: TRAINING, INFORMATION...)]

As already mentioned, pursuant to the law, the internal rules for the responsible for reporting persons (or persons in charge of reporting) shall include the rules for the training of officials within the specialized units when the law states that such units should be created, as it is the case with banks.

In compliance with the Rules for the implementation of the AML Act, the persons responsible for reporting are obliged to ensure self-sustained training of its employees within the specialized units and the rest of the employees with regard to their activities on the prevention of money laundering and the implementation of the AML legislation.

These obligations are realized in practice by the banks.

## CZECH REPUBLIC

Czech Banking Association

### [ANTI-MONEY LAUNDERING /CTF LEGISLATION]

The first Czech AML Act N°61/1996 Coll. was drawn up in 2005. It has been amended eleven times (in the connection with the FATF and EU requirements) and in 2007 a completely new AML/CFT act was drawn up – “The Act N°253/2008 Coll. concerning some measures against legitimisation of proceeds of crime and financing of terrorism” (hereinafter the **AML/CFT act**). This act came into effect on 5 June 2008 and will enter into force on 1<sup>st</sup> September 2008.

### [PENALTIES IN NATIONAL LAW FOR FAILURE TO RESPECT THE NATIONAL PROVISIONS OF THE DIRECTIVE]

Penalties in volume up to 50.000.000,-CZK, forfeiture of property, suspension of banking business licence.

### [CENTRAL AUTHORITY FOR REPORTING]

The Financial Analytical Unit of the Ministry of Finance acts as the central authority for reporting (financial intelligence unit). This unit was established on 1 July 1996. It is responsible for receiving, collecting and analysing suspicious transaction reports coming from obliged entities. It has investigative powers and, in the case of failure to implement or in the case of any breach of obligations under money laundering legislation, FAU is empowered to deliver to the appropriate licensing authority (Czech National Bank) a motion to repeal the licence of the person in question. The licensing authority shall, within thirty days of the motion, inform FAU on measures taken and on its decision *in re*?. The central authority for reporting (Financial Analytical Unit) is not, however, mandated to withdraw the banking licence. FAU lodges the complaint with the law enforcement authorities in the case of suspicion of crime.

### [PERSONS RESPONSIBLE FOR REPORTING]

#### **Section 22 of the AML/CFT act**

##### **Contact Person**

- (1) The obliged entity shall appoint one of its employees to report under Section 18 and to maintain regular contacts with the Ministry, unless it decides to entrust such responsibilities to its statutory body. The Ministry shall be, with no undue delay, notified

of such appointment and informed of the name, surname, position, and telephone number and email address of the appointee.

- (2) No credit or financial institution shall appoint a member of its statutory body as a contact person unless it is necessary with regards to its size, management structure, or number of employees.
- (3) No credit or financial institution shall appoint as a contact person, a member of staff responsible for performing or settlement of its transactions, or an employee participating in the performance of internal audit.
- (4) The obliged entities which decide not to entrust the contact responsibilities to its statutory bodies shall provide for a direct contact between the appointed contact person on one side, and its statutory and supervisory bodies, on the other.

[BUSINESS COVERED BY THE LEGISLATION (WHICH SPECIFIC PERSONS: NOTARIES, LAWYERS...)]

## ***Section 2 of the AML/CFT Act***

**For the purposes of the AML/CFT Act, the obliged entity shall be understood as:**

- a) A credit institution in a form of :
  - a bank,
  - a cooperative savings or credit union,
  - an electronic money institution,
  - a person authorised to issue electronic money based on a licence in keeping with legislation that provides guidance for the issue, and use of electronic means of payment.
- b) A financial institution, which is an undertaking other than a credit institution, such as:
  - the Central Depository, the entity keeping a register related to the Central Register of Securities maintained by the Central Depository, the entity keeping an independent register of investment instruments, the entity keeping a register related to the independent register of investment instruments;
  - an administrator of investment tools market;
  - a person licensed to provide investment services with the exception of an investment broker;
  - an investment company, an investment fund, or a pension fund;
  - a person entitled to issue or administer non-cash means of payment;
  - a person authorized to provide or trade with leasing, guarantees, credit or loans;

- a person authorized to broker savings, leasing, credit or loans;
  - an insurance or re-insurance company, an insurance agent and an insurance settlement agent when performing activities related to the life insurance, with the exception of an insurance agent whose liability for damage is borne by his contracting insurance company;
  - a legal or natural person authorised to buy and trade in debt and receivables;
  - a person licensed to perform exchange of foreign currency or wireless foreign currency transfers pursuant to the Foreign Currency Act;
  - a person licensed to provide or broker payment services, including money services, or postal services intended to transfer money;
  - a person licensed to provide consultancy services to private business in matters concerning equity, business strategy, merge, or acquisition;
  - a person providing services of financial brokerage;
  - a person providing services of safekeeping of valuables.
- c) A holder of a licence to operate betting games in casinos in keeping with the Act on lotteries and other similar games,
- d) A legal or natural person authorised to act as a real estate trader or broker,
- e) An auditor, tax advisor, or chartered accountant,
- f) A court executor when performing other activities of an executor pursuant to the Executor proceedings as well as safekeeping of money, securities, or other valuables,
- g) A public notary providing safekeeping notarial services; a lawyer or a public notary offering the service of safekeeping money, securities, or other client's valuables; or a lawyer or a public notary required by the client to represent him or to act on his behalf in the following:
- buying or selling real estate, a business entity, or its part;
  - managing of client assets, such as money, securities, business shares, or any other assets, including representation of the client or acting on his account in relation to opening bank accounts in banks or other financial institutions or establishing and managing securities accounts; or
  - establishing, managing, or controlling a company, business group, or any other similar entrepreneurial entity regardless of its status of a natural/legal person as well as receiving and gathering of money or other valuables for the purpose of establishing, managing, or controlling such entity; or
  - providing services of encashment, payments, transfers, deposits, or withdrawals in wire or cash transactions, or any other conduct aimed at or directly triggering movement of money;

- h) A person not guided by letters a) to g), providing the following professional services to another person:
  - establishing legal persons;
  - acting as a statutory body or its member, or acting as person appointed to act in the name of or on behalf of a legal person, or another person in a similar position, should such service be only temporary and should it be related to establishing and administration of a legal person;
  - providing a business location, address, and possibly other related services to another legal person;
  - acting as an appointed shareholder on behalf of another person, who is not a business and whose securities have been accepted for trading at a regulated market and which is subject to information disclosure requirements equal to those enforced by the EU legislation; or
  - acting in his/her name of or on his/her behalf in activities stipulated in letter g),
- i) A person providing services under letter h) in a framework of a trust or any other similar contractual relationship under foreign law;
- j) A person licensed to trade in items of cultural heritage, items of cultural value, or to act as intermediary in such services;
- k) A person licensed to trade in used goods, act as intermediary in such trading, or receive used goods in pawn.

**Legal or natural person acting in the exercise of his/its professional activities, such as:**

- l) A foreign legal or natural person as stipulated by Subsection 1, operating in the territory of the Czech Republic via its branch or subsidiary; such person meets the definition of an obliged entity in the extent of activities performed by such branch or subsidiary;
- m) A foreign national operating in the territory of the Czech Republic should he perform activities stipulated in Subsection 1;
- n) The Securities Centre;
- o) An entrepreneur not listed in Subsection 1, should he receive payments in cash in an amount of EUR 15,000 or more; or
- p) A legal person which is not a business should it be licensed to provide, in a form of a service, any of the activities stipulated in Subsection 1, or should it receive payments in cash in an amount of EUR 15,000 or more.

A person not performing activities stipulated in Subsection 1 as a professional business activity, with the exception of a person listed in Subsection (2d) and (2e), is not considered to be an obliged entity.

[PREDICATE OFFENCES COVERED]

In the Czech Republic any criminal act having proceeds is the predicate offence for money laundering (all crime approach).

[IDENTIFICATION]

**a. Definition (e.g.: PEPs, beneficial owner, thresholds...)**

**Section 4 (5) of the AML/CFT act**

Politically exposed person shall mean:

- a) a natural person in a prominent public position and with nation-wide responsibilities, such as a head of state, a head of government, a minister, deputy or assistant minister, a member of the parliament, a member of a supreme court, a constitutional court or another high-level judicial body decisions of which are not subject to further appeal, except in exceptional circumstances, a member of a court of auditors or a central bank board, a high-ranking military officer, a member of an administrative, supervisory, or management board of a state-owned business, an ambassador or chargé d'affaires, or a natural person, having similar responsibilities on a Community or international level; all the above for the entire period of the position and for one year after the termination of such position, and provided the person:
- has a residence outside the territory of the Czech Republic; or
  - holds such important public position outside the Czech Republic,
- b) a natural person, who
- is the spouse, partner equivalent to the spouse or a parent of the person under a),
  - is a son or a daughter of the person under letter a) or a spouse or a partner of such a son or daughter (a son or daughter in law),
  - is a business partner or a beneficial owner of the same legal person, a trust, or any other business entity under a foreign law, as the person under letter a) or is known to the obliged entity as a person in a close business relationship with a person under letter a); or
  - is a business partner or a beneficial owner of the same legal person, a trust, or any other business entity under a foreign law known to have been established in benefit of a person under letter a).

Beneficial owner shall mean either:

- a) an entrepreneur as:
  - a natural person, having real or legal direct or indirect control over the management or operations of such entrepreneur, indirect control shall mean control via other person or persons;
  - a natural person, holding in person, or in contract with a business partner, or partners with more than 25% of the voting rights of such a entrepreneur; disposing of voting rights shall mean having an opportunity to vote based on one's own will regardless of the legal background of such right or an opportunity to influence voting by other persons;
  - natural persons acting in concert and holding over 25% of the voting rights of such a entrepreneur; or
  - a natural person, which is, for other reasons, a real recipient of such entrepreneur's revenue,
  
- b) a foundation or a foundation fund as:
  - a natural person, which is to receive at least 25% of the distributed funds; or
  - a natural person or a group of persons in whose interest a foundation or a foundation fund had been established or whose interests they promote, should the beneficiary of such foundation or a foundation fund yet to be determined,
  
- c) a natural person, in case of an association under *lex specialis*, public service organization, or any other person and a trusteeship or any other similar legal arrangement under a foreign law, who:
  - holds over 25% of its voting rights or assets,
  - is a recipient of at least 25% of the distributed assets, or
  - in whose interest they had been established or whose interests they promote, should their future beneficiary yet to be determined.

**b. Identification threshold amount**

**Section 4 (5) of the AML/CFT act**

**Identification Requirement**

(1) The obliged entity, should it be a party to a transaction exceeding EUR 1,000, shall always identify the client prior to the transaction, unless stipulated otherwise by this Act.

(2) The obliged entity shall, without regard to the limit stipulated in Subsection 1, always identify the client should it concern the following:

- a suspicious transaction;
- an agreement to enter into a business relationship;
- an agreement to establish an account; an agreement to make a deposit into a deposit passbook or a deposit certificate; or an agreement to make any other type of deposit;
- an agreement to use a safety deposit box or an agreement on custody;
- a life insurance contract, should the client have a right to pay extra premiums above the agreed limit of the one-off or regular premium payments;
- a purchase or reception of cultural heritage, items of cultural value, used goods or goods without a receipt of origin to further trade in such goods, or reception of such items in pawn; or
- withdrawal of a cancelled bearer passbook final balance.

(3) The obliged entity shall, at the latest on the day of the payment, identify the individual entitled to receive the life insurance settlement.

*(There are some cases, e.g. when an agreement to enter into a business relationship, an agreement to establish an account etc., when identification is made without regard to the stipulated limit.)*

**c. Identification at a distance (non face to face)**

**Section 10 of the AML/CFT act**

**Customer Due Diligence Performed by a Public Notary, or a Regional or Municipal Authority**

(1) Should the first client identification by the obliged entity under Section 8(1) be, for serious reasons, impossible, such identification may be, upon request of either a client or the obliged entity, performed by a public notary, a regional office, or a local authority in a municipality exercising devolved powers of the State.

- (2) A public notary or an office in Subsection 1 shall take a record of such identification; the record, which becomes an official document, shall bear the following properties:
- the name of the person performing the identification, name of the requesting person, and purpose of such identification;
  - client identification data;
  - a declaration of the identified natural person, the person acting on behalf of the identified legal person or a proxy, on the purpose and correctness of the identification performed, eventually on reservations to such identification;
  - the place and date of the record and the place and date of the identification, if they differ;
  - the signature of the identifying person, an official stamp, or a serial number in the log of identification records.
- (3) As an appendix to the identification record, the obliged entity shall make copies of relevant parts of documents used for the identification and bearing identification data, type and serial number of the ID, issuing country and institution, and validity as well as, with requests filed in writing, a copy of the request. Should this procedure be used to identify a proxy, the power of attorney or its certified copy shall also be attached as an appendix. All appendices shall be attached to the identification record to make a complete file.
- (4) All copies shall be legible and capable of storage for the period stipulated in Section 16. The file of copies shall include a copy of the image of the identified person in his ID which allows for visual identification.
- (5) Both a public notary and an institution under Subsection 1 shall keep an internal log of identification records, in which it shall document the following:
- a serial number and date of the record;
  - the following identified person's data:
    - name, surname, permanent or other residence, birth registration number or date of birth of the identified natural person or natural person acting on behalf of the identified legal person;
    - in case of a legal person, its business or corporate name, the business name, an appendix to the business name or any other identification features, place of business, and business registration number,
  - the purpose of identification.
- (6) The identification record log is kept on a calendar year basis and complete logs shall be stored for a period of ten years.

**Section 11 (4) and (7) of the AML/CFT act**

In the event of a remote agreement on financial services under the Civil Code, the obliged entity shall identify the client as follows:

- a) the first payment from this agreement shall be made *via* an account kept on the client's name in a credit institution or a foreign credit institution operating in the EU or EEA;
- b) the client shall submit to the obliged entity a copy of a document verifying the existence of an account under letter a) above, together with copies of the relevant parts of his ID and at least one more identification document from which the obliged entity may determine the client's identification data, type and serial number of such IDs, issuing country or institution, and validity. Such copies shall be made in line with requirements under Section 10(4).

In cases under Subsections 1, 4, 5 and 6, the obliged entity shall verify that all conditions required have been met and that none of the clients, products, or transactions represent a risk of legitimisation of proceeds of crime or financing of terrorism. In case of doubt, no exceptions shall be applied.

**Section 12 of the AML/CFT act**

**Common Provisions to Identification under Section 10 and Section 11**

In case of identification and other steps under Section 10 or Section 11(4) and 11(6), all identification data and other information and documents listed therein shall be deposited with the obliged entity prior to the transaction.

**d. Outsourcing of identification to third parties**

**Section 11 (1-3) and (5-6) of the AML/CFT act**

**Transfer of Identification**

(1) The obliged entity may decide not to identify a client or seek information on the purpose and nature of a transaction or a business relationship under Section 9(2a) and identify a beneficial owner under Section 9(2b), should these steps have already been performed by:

- a credit or financial institution, with the exception of a financial institution under Section 2(1b), points 10 and 11; or
- a foreign credit or financial institution, with the exception of a person licensed to exchange foreign currency or a financial institution providing transfers of money abroad, should it be located in the territory of a country imposing and enforcing similar identification, due diligence, and data keeping requirements, and be subject to compulsory business licensing or registration and supervision to on and off-site control of its general performance as well as individual transactions.

(2) The obliged entity acting in keeping with Subsection 1 shall make sure that it will receive, from the credit or financial institution, or a foreign credit or financial institution which had performed the identification, all relevant documents, including copies of all documents used in client identification, all data indicating the purpose and nature of the business transaction, and information on the identity of the beneficial owner. The credit or financial institution shall, upon consent of the person identified and without undue delay, submit all information including copies of the document here above; to another obliged entity should such person decide to rely on it for the client identification.

(3) The obliged entity shall refuse the client identification information, data indicating the purpose and nature of the business transaction, and information on the identity of the beneficial owner under subsections 1 and 2, should it have a reason to doubt the correctness or completeness of such information.

(5) The credit or financial institution may not perform the client identification and seek the data indicating the purpose and nature of the business transaction under Section 9(2a), and information on the identity of the beneficial owner under Section 9(2b) should these steps have been undertaken prior to the transaction by a person acting on its behalf, and on its account, and bound by its internal regulations, and should such credit or financial institution bear responsibility for damages caused by such a person. All information including copies of documents under the first sentence here above shall be kept at the obliged entity.

(6) The credit or financial institution, when providing investment services, may decide not to perform the client identification, and seek the data indicating the purpose and nature of the business transaction under Section 9(2a), and information on the identity of the beneficial owner under Section 9(2b), should these steps have been performed by an investment broker in line with this Act and its internal regulations. The obliged entity shall bear responsibility for such steps as if it had been its own performance.

**e. Means of identification**

**Section 4 (6) of the AML/CFT act**

For the purposes of this Act, an identification document shall mean an ID issued by the public administration and bearing the holder's name, surname, and date of birth together with an image and potentially other identification features allowing for the identification of the bearer as the true holder.

**f. Source of information (e.g.: public register for the identification of beneficial owner)**

Companies Register (legal persons), Trade Register (physical persons).

## [PRODUCTS AND TRANSACTIONS CHARACTERISED BY A HIGH/LOW RISK OF MONEY LAUNDERING]

### **Section 6 of the AML/CFT act**

For the purposes of this Act, suspicious transaction shall mean a transaction the circumstances of which lead to a suspicion of legitimisation of proceeds of crime or financing of terrorism or any other unlawful activity. The following client activities shall be perceived as suspicious:

- a) cash deposits immediately followed by withdrawals or transfers to other accounts;
- b) numerous transactions performed in one day or in a short period of time and not typical of the given client;
- c) a number of various accounts opened by the given client which are in obvious discrepancy with his business activities and wealth;
- d) transactions that obviously make no economic sense;
- e) assets handled by the client which are in obvious discrepancy with his business activities and wealth;
- f) an account which is not used for the purposes for which it had been opened;
- g) client performance which seems to aim at concealing his or the beneficial owner's real identity;
- h) the client or the beneficial owner who are nationals of a country which does not enforce, or fails to fully enforce, measures to combat legitimisation of proceeds from crime and financing of terrorism; or
- i) client identification data the correctness of which the obliged entity has reasons to doubt.

A transaction shall always be perceived as suspicious, should:

- a) the client or the beneficial owner be a person against whom the Czech Republic had imposed international sanctions under the Act on international sanctions;
- b) the goods or services dealt in the transaction fall in the category against which the Czech Republic had imposed international sanctions under the Act on international sanctions; or
- c) the client refuse to reveal identification data of the person he is representing or to undergo the due diligence process.

## [EXISTING GUIDELINES TO THE BANKING INDUSTRY]

The Czech National Bank passes implementing regulations determining requirements for implementing and enforcing internal procedures by selected obliged entities.

## [GENERAL FEEDBACK (NEW MODUS OPERANDI, TRENDS, REAL CASES, etc)]

The Czech financial intelligence unit (the Financial Analytical Unit of the Ministry of Finance) shall maintain and publish at least once a year on its website, statistical reports of effectiveness and results of measures against the legitimisation of proceeds of crime and financing of terrorism, including new ML/TF trends and typologies. What is more, FAU published the guide “100 Sanitized Cases of Money Laundering” and distributed it to the banking sector as well as the training CD-rom on combating money laundering.

## [PURPOSES FOR WHICH THE FEEDBACK INFORMATION MAY BE USED]

The feedback is important especially for obliged entities. They can, on the basis of good feedback, set up for example new filters for monitoring of transactions.

## [PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK STAFF IN THE EVENT OF NOTIFICATION) OF THE INSTITUTIONS OR PERSONS COVERED BY THIS DIRECTIVE ]

### **Section 18 (3) of the AML/CFT act**

The suspicious transaction report shall not reveal any information about the obliged entity's employee or contractor who disclosed the suspicious transaction (section 18, article 3 of new Czech AML Act).

## [CONSERVATION OF RECORDS AND DOCUMENTS]

### **Section 16 of the AML/CFT act**

#### **Obliged Entity Record Keeping**

(1) The obliged entity shall, for the period of 10 years after having terminated its business relationship with the client, keep record of all identification data taken under Section 8(1) and 8(2) or in keeping with the directly applicable EU Regulation stipulating the obligation to accompany transfers of funds with information on the payer, copies of documents submitted for identification (should there be any), records of the first identification (name and date), documents justifying potential derogations from identification and due diligence under Section 13, and, in case of representation, the original or a certified copy of the power of attorney.

(2) The obliged entity shall, for the period of 10 years after the transaction or after having terminated its business relationship with the client, keep record of all data and documents on transfers requiring identification.

(3) The obliged entity stipulated in Section 2(1j) and 2(1k) shall keep record of all data and documents for the period of at least 10 years after the transaction, or after having terminated its business relationship with the client should such transaction or relationship reach or exceed EUR 10 000; in other cases it shall keep its records for a period of 5 years.

(4) The statutory period under Subsections 1 to 3 shall commence on the first day of the calendar year following the calendar year in which the obliged entity performed the last transaction.

[STEPS TAKEN TO INCREASE AWARENESS OF THE PHENOMENON OF MONEY LAUNDERING (E.G.: TRAINING, INFORMATION...)]

The obliged entities shall organize, at least once in 12 calendar months, training of all members of its staff who may, in the course of their professional obligations, come in contact with suspicious transactions. All appointees to such positions shall be trained *prior* to taking their appointment.

The training shall concentrate on types and features of suspicious transactions and steps taken in detecting such transactions. The obliged entity shall regularly update such trainings.

The Czech financial intelligence unit (the Financial Analytical Unit of the Ministry of Finance)) shall maintain and publish at least once a year on its website, statistical reports of effectiveness and results of measures against the legitimisation of proceeds of crime and financing of terrorism. Law enforcement authorities shall provide the Ministry of finance on a regular basis with summary statistics on matters relating to the legitimisation of proceeds of crime and financing of terrorism.

FAU also regularly organizes trainings for ML reporting officers by means of the chambers and the associations of obliged entities. Moreover, it published the guide “100 Sanitized Cases of Money Laundering” and distributed it to the banking sector as well as the training CD-rom on combating money laundering.

### [ANTI-MONEY LAUNDERING /CTF LEGISLATION]

Current Danish regulation on money laundering and financing of terrorism (AML) is included in

- The Act on Measures to Prevent Money Laundering and Financing of Terrorism
- The Criminal Code
- The Customs Act
- The Act on Gambling Casino and
- EU regulations.

The Act on Measures to Prevent Money Laundering and Financing of Terrorism is originally from 1993 – implementing the first Money Laundering Directive (91/308). Due to 9/11, the following second EU Directive on Money Laundering (2001/97) and the FATF special recommendations on terrorist financing, the AML was substantially amended in 2002.

The current Act on Measures to Prevent Money Laundering and Financing of Terrorism is from 26 February 2006 implementing the third EU Money Laundering Directive (2005/60) and FATF 40 recommendations. The Act replaced the Act from 1993 and entered into force on 1 March 2006.

The Act has been amended several times to comply with IMF-standards and recent FATF recommendations.

### [PENALTIES IN NATIONAL LAW FOR FAILURE TO RESPECT OF THE NATIONAL PROVISIONS TO THE DIRECTIVE]

The Act states that intentional or grossly negligent violation of the provisions of the Act, including the obligation to report suspected money laundering or financing of terrorism, is subject to a fine, unless more severe punishment is incurred under the regulations of the Criminal Code, for instance sec. 290 (receiving stolen goods) and sec. 114 b (supporting terrorism).

In the event of particularly gross or extensive intentional violations the penalty may be increased to imprisonment of up to six months.

### [CENTRAL AUTHORITY FOR REPORTING]

The Money Laundering Secretariat – a unit under the Public Prosecutor for Serious Economic Crimes (the FIU) - receives reports of suspected laundering of proceeds of crime or financing of terrorism. The FIU was established in 1993.

## [PERSONS RESPONSIBLE FOR REPORTING]

Generally the management of the bank is responsible for providing written procedures for all significant areas of activity and according to the Act on Money Laundering the management shall provide for an internal reporting system specifying which person or department in the bank's reporting hierarchy the employee is to report to as regards a suspicion of money laundering and the person/department of the bank with the overall responsibility for notifying the Money Laundering Secretariat.

## [BUSINESS COVERED BY THE LEGISLATION (WHICH SPECIFIC PERSONS: NOTARIES, LAWYERS...)]

- 1) Banks
- 2) Mortgage-credit institutions
- 3) Investment companies
- 4) Investment management companies
- 5) Life assurance companies and lateral pension funds (nationwide occupational pension funds).
- 6) Savings undertakings.
- 7) Electronic money institutions.
- 8) Insurance brokers, when they act in respect of life assurance or other investment-related insurance activities.
- 9) Foreign undertakings' branches in Denmark, carrying out activities under nos. 1-8.
- 10) Investment associations and special-purpose associations, collective investment schemes, restricted associations, innovation associations and hedge associations.
- 11) Undertakings and persons that commercially carry out activities involving currency exchange or transfer of money and other assets.
- 12) Other undertakings and persons that commercially carry out one or more of the activities mentioned in annex 1.
- 13) Lawyers when they participate by providing assistance in the planning or execution of transactions for their clients concerning
  - a. purchase and sale of real property or undertakings,
  - b. managing their clients' money, securities, or other assets,
  - c. opening or managing bank accounts, savings accounts, or securities accounts,
  - d. raising the necessary capital for establishment, operation, or management of undertakings,
  - e. establishing, operating, or managing undertakings, or
  - f. providing other business advice.

- 14) Lawyers when they, on behalf of their client and at said client's expense, carry out a financial transaction or a transaction concerning real property.
- 15) State-authorized public accountants and registered public accountants.
- 16) Authorized estate agents.
- 17) Undertakings and persons that otherwise commercially supply the same services as the groups of persons mentioned in nos. 13-16, including tax advisors and external accountants.
- 18) Providers of services for undertakings, cf. section 3, no. 5.
- 19) Danmarks Nationalbank (Denmark's central bank), insofar as it carries out activities corresponding to those of the institutions specified in no. 1.

## [PREDICATE OFFENCES COVERED]

The Danish AML does not provide for a list of predicate offences. In principle all crimes are covered if there is a suspicion that a customer's transaction or enquiry is or has been associated with money laundering or financing of terrorism.

### **Identification**

#### **a. Definition (e.g.: PEPs, beneficial owner, thresholds...)**

The Danish AML has implemented the definitions in the third Money laundering Directive, except the customer due diligence threshold of 15.000 Euro. Instead the Act prohibits retailers and auctioneers to receive cash payments of DKK 100,000 or more irrespective of whether payment is effected in one instance or as several payments that seem to be mutually connected.

The definition of PEPs is supplemented by the Directive on implementing measures.

#### **b. Identification threshold amount**

In general the Danish AML does not set limits above which transactions require special attention.

However, for customers with single transactions (occasional customers) banks are required to meet the requirements of the Act, including proof of identity, for each transaction of amounts corresponding to DKK 100,000 or more. If the value of a transaction is not known at the time of commencement of said transaction, proof of identity shall be demanded as soon as the bank suspects that the transaction concerned is of the type covered by subsection.

## [MEANS OF IDENTIFICATION]

The Danish AML does not prescribe the use of specific documents of identification, but the information concerning identity must be checked on the basis of reliable identification documents – without these being further specified.

Primary documents of identification consist of official photographic identification e.g.: EU driving licence and valid passport. If the customer is in the possession of a driving licence or a passport but the identification does not take place on the basis of one of these documents the

bank shall record and store why the identification procedure was not based on the said documents.

The identification procedure for legal person shall be based on a registration certificate issued by The Danish Commerce and Companies Agency.

## [SOURCE OF INFORMATION (E.G.: PUBLIC REGISTER FOR THE IDENTIFICATION OF BENEFICIAL OWNER)]

Denmark does not have any official register for identification of beneficial owners. However, information on the beneficial owners of a limited company can be found in the company's financial statements, which can be obtained from the Danish Commerce and Companies Agency. The financial report lists all shareholders holding more than 5% ownership.

## [PRODUCTS AND TRANSACTIONS CHARACTERISED BY A HIGH/LOW RISK OF MONEY LAUNDERING]

Based on a risk assessment, banks must in a number of cases make further requirements of the proof of identity of customers and customer due diligence in situations which in themselves increase the risk of money laundering and financing of terrorism.

The AML contains a number of examples of such high risk customers. These include:

- Customers who are not physically present to prove their identity, including Internet customers
- Cross border correspondent-bank relations
- PEPs - Politically exposed persons
- Others, for example persons who have previously been under suspicion.

## [EXISTING GUIDELINES TO THE BANKING INDUSTRY]

The Danish Financial Supervisory Authority issued in 2006 general guidelines on Measures to Prevent Money Laundering and Financing of Terrorism.

Previously The Danish Bankers Association already in 1993 issued industry specific guidelines on Money Laundering and Terrorism including indicators in cooperation with the FIU.

## [GENERAL FEEDBACK (NEW MODUS OPERANDI, TRENDS, REAL CASES, ETC.)]

The FIU gives a general feedback and information on new trends at regular meetings in the Danish Banker Association's AML-group consisting of representatives from the major banks, the Association, the FSA and the FIU. The group discusses all questions relating to money laundering including specific cases and new trends.

Individual feedback may be given by the FIU, if investigative considerations do not contradict this, to the notifying bank about the status of the matter, including whether a charge has been

made, and may inform about deletion from the money laundering register at the FIU, and about a final decision, on conviction possibly in the form of a judgment or a transcript of a judgment.

## [PURPOSES FOR WHICH THE FEEDBACK INFORMATION MAY BE USED]

General feedback (summarised feedback) may be used for employee training. Specific feedback is confidential information and must only be used for the bank's consideration on handling and maintaining the customer relationship in question.

## [PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK STAFF IN THE EVENT OF NOTIFICATION OF THE INSTITUTIONS OR PERSONS COVERED BY THIS DIRECTIVE)]

There are no specific provisions on protection of employees. However, the reporting bank employee who has direct customer relationship need not sign or be named on the notification sent to the FIU and which may come to the knowledge of the suspected customer during the trial.

Banks making notifications in good faith and suspension of transactions according to the AML does not incur any liability on the bank, its employees or management.

## [CONSERVATION OF RECORDS AND DOCUMENTS]

Banks shall store identity information for no less than five years after the customer relationship has ceased. Documents and records concerning transactions shall be stored for at least five years after the performance of the transactions.

## [STEPS TAKEN TO INCREASE AWARENESS OF THE PHENOMENON OF MONEY LAUNDERING (E.G.: TRAINING, INFORMATION...)]

Banks are required to draw up written internal rules that clearly describe the obligation of the employees under the AML.

In addition the Danish Bankers association has issued training material, including e-learning education, for bank employees and a booklet concerning identification procedures.

### [ANTI-MONEY LAUNDERING /CTF LEGISLATION]

The AML/CTF legislation in Estonia is regulated by various legal acts. The main of which are the following:

- Money Laundering and Terrorist Financing Prevention Act, entered into force on 28.01.2008, (with applied amendments 10.07.2008) thus fully implementing European Parliament and Council directives 2005/60/EC and 2006/70/EC.
- Several directives of Interior ministry and ministry of Finance.
- Administrative acts of Financial Intelligence Unit, FSA recommendation guidelines.

### [PENALTIES IN NATIONAL LAW FOR FAILURE TO RESPECT OF THE NATIONAL PROVISIONS TO THE DIRECTIVE]

The Financial Intelligence Unit issues precepts and other administrative acts in order to perform the functions arising from law.

In the event of failure to comply with an administrative act, the Financial Intelligence Unit may impose a coercive measure pursuant to the procedure provided for in the Substitutive Enforcement and Penalty Payment Act. The upper limit for a penalty payment for failure to comply with an administrative act is 20,000 kroons (1278 EUR) for the first occasion and 80,000 kroons (5113 EUR) for each subsequent occasion.

According to the Penal Law Money laundering is punishable by a pecuniary punishment or up to 5 years' imprisonment.

The same act, if committed:

- 1) by a group;
- 2) at least twice;
- 3) on a large-scale basis, or
- 4) by a criminal organisation,

is punishable by 2 to 10 years' imprisonment.

An act, if committed by a legal person, is punishable by a pecuniary punishment.

An act provided for in subsection (2) of this section, if committed by a legal person, is punishable by a pecuniary punishment or compulsory dissolution.

A court may apply confiscation of an property which was the direct object of the commission of

an offence provided for in this section.

For the criminal offence the court shall impose extended confiscation of assets or property acquired by the criminal offence

## [CENTRAL AUTHORITY FOR REPORTING]

Estonian Financial Intelligence Unit (FIU) is an independent structural unit of the Central Criminal Police. The Financial Intelligence Unit analyses and verifies information about suspicions of money laundering or terrorist financing, takes measures for preservation of property where necessary and immediately forwards materials to the competent authorities upon detection of elements of a criminal offence.

All persons who suspect that a transaction may be connected with either money laundering or terrorist financing are encouraged to notify of suspicious transactions. Since January 2008 it is possible to send the notification to FIU electronically by using the digital format on the website of the Financial Intelligence Unit.

## [BUSINESS COVERED BY THE LEGISLATION (WHICH SPECIFIC PERSONS: NOTARIES, LAWYERS...)]

- credit institutions;
- financial institutions;
- organisers of games of chance;
- persons who carry out or act as intermediaries in transactions with real estate;
- traders for the purposes of the Trading Act, if a cash payment of no less than 200,000 kroons or an equal amount in another currency is made to the trader, regardless of whether the financial obligation is performed in the transaction in a lump sum or in several related payments, unless otherwise provided by law;
- pawnbrokers;
- auditors and providers of accounting services;
- providers of accounting or tax advice services;
- providers of trust and company services.
- Legislation applies to notaries public, attorneys, bailiffs, trustees in bankruptcy, interim trustees in bankruptcy and providers of other legal services if they act in the name and on account of a customer in financial or real property transactions. This Act also applies to the specified persons if they guide planning a transaction or perform an official act, which concerns:

- the purchase or sale of immovables, enterprises or companies;
- the management of the customer's money, securities or other property;
- the opening or managing of bank or security accounts;
- the acquisition of funds necessary for the foundation, operation or management of companies;
- the foundation, operation or management of trusts, companies or other similar entities.

[IDENTIFICATION]

## **General application of due diligence measures**

An obligated person shall apply following due diligence measures before establishment of any business relationship or entering into any transaction

- 1) identification of a customer or a person participating in a transaction on the basis of documents and data submitted by him or her and verification of the submitted information on the basis of information obtained from a reliable and independent source;
- 2) identification and verification of a natural person or a representative of a legal person and the right of representation;
- 3) identification of the beneficial owner, including gathering information about a legal person, trust, civil law partnership or other contractual legal arrangement on the basis of information provided in pre-contractual negotiations or obtained from another reliable and independent source;
- 4) acquisition of information about a business relationship and the purpose of a transaction.

If a financial obligation is performed in a transaction by way of several related payments and the total amount of these payments is unknown, the person must be identified and verified as soon as the exceeding the amount of 200,000 kroons.

An obligated person shall apply any and all due diligence measures, but may choose the appropriate scope of application of the due diligence measures based on the nature of the business relationship or transaction or the risk level of the person or customer participating in the transaction or official act.

Upon application of the due diligence measures specified in clauses an obligated person has the right to rely on information received by the obligated person in a format which can be reproduced in writing from a credit institution registered in the Estonian commercial register or from a branch of a foreign credit institution or from a credit institution who has been registered

or whose place of business is in a contracting state of the European Economic Area or a third country where requirements equal to those provided in this Act are in force.

## **Politically exposed person**

(1) A politically exposed person is a natural person who performs or has performed prominent public functions, their family members and close associates. A person who, by the date of entry into a transaction, has not performed any prominent public functions for at least a year, or the family members or close associates of such person are not considered a politically exposed person.

(2) For the purposes of this Act, a person performing prominent public functions is:

- a head of state, head of government, minister, and deputy or assistant minister;
- a member of parliament;
- a justice of a supreme, constitutional or another court the judgments of which can be appealed to only in exceptional circumstances;
- a member of the supervisory board of a state audit institution or central bank;
- an ambassador, chargé d'affaires and senior officer of the Defence Forces;
- a member of a directing, supervisory or administrative body of a state company.

(3) The provisions of clauses (2) 1)-5) includes positions of the European Union and other international organisations.

(4) A family member of a person performing prominent public functions is:

- his or her spouse;
- a partner equal to a spouse under the law of the person's country of residence or a person who as of the date of entry into the transaction had shared the household with the person for no less than a year;
- his or her children and their spouses or partners within the meaning of clause 2);
- his or her parent.

(5) A close associate of a person performing prominent public functions is:

- a natural person who has a close business relationship with a person performing prominent public functions or with whom a person performing prominent public functions is the joint beneficial owner of a legal person or contractual legal arrangement;
- a person who as a beneficial owner has full ownership of a legal person or contractual legal arrangement, which has in fact been founded for the benefit of the person performing prominent public functions.

## **Beneficial owner**

(1) A beneficial owner is a natural person who, taking advantage of his or her influence, exercises final control and in whose interests or favour or on whose account a transaction or act is performed. A beneficial owner is a natural person who has or exercises final control over management of a company:

- by having over 25 percent of shares or voting rights through direct or indirect shareholding or control, including in the form of bearer shares;
- otherwise exercising control over management of a legal person.

(2) A beneficial owner is also a natural person who, to the extent of no less than 25 percent determined beforehand, is a beneficiary of a legal person or civil law partnership or another contractual legal arrangement, which administers or distributes property, or who exercises control over the property of a legal person, civil law partnership or another contractual legal arrangement to the extent of no less than 25 percent.

(3) A beneficial owner is also a natural person who, to an extent not determined beforehand, is a beneficiary of a legal person or civil law partnership or another contractual legal arrangement, which administers or distributes property, and in whose interests a legal person, civil law partnership or another contractual legal arrangement is set up or operates.

[PRODUCTS AND TRANSACTIONS CHARACTERISED BY A HIGH/LOW RISK OF MONEY LAUNDERING]

## **Conditions of application of simplified due diligence measures**

(1) An obligated person may apply simplified due diligence measures if a person or customer participating in a transaction entered into in economic or professional activities or in an official act is:

- a legal person governed by public law founded in Estonia;
- a governmental authority or another authority performing public functions in Estonia or a contracting state of the European Economic Area;
- an authority of the European Community;
- a company of a contracting state of the European Economic Area or a third country, which is subject to requirements equal to those provided for in this Act and whose securities are traded in a regulated securities market in one or several contracting state of the European Economic Area;
- a credit or financial institution, a credit or financial institution located in a contracting state of the European Economic Area or a third country, which in the

country of location is subject to requirements equal to those provided for in this Act and the performance of which is subject to state supervision.

(2) An obligated person may apply the simplified due diligence measures with regard to the beneficial owners of an official account opened by a notary public or bailiff of a contracting state of the European Economic Area or third country, provided that the official account is subject to due diligence measures which are in compliance with the international standards for prevention of money laundering and terrorist financing, state supervision is exercised over adherence to these requirements and the notary public or bailiff has and preserves information about the identity of the beneficial owner.

An insurer or insurance broker may apply simplified due diligence measures if:

- a life assurance contract is made whereby the annual assurance premium does not exceed 15,000 kroons or a single premium does not exceed 35,000 kroons;
- a pension insurance contract is made which does not provide for the right of withdrawal or cancellation and which cannot be used as loan collateral;
- a transaction is entered into in the framework of a superannuated pension scheme or another scheme allowing for such pension benefits whereby insurance premium is debited from wages and the terms and conditions of the pension scheme do not allow for assignment of the rights of a participant in the scheme.

An obligated person may apply simplified due diligence measures in a transaction if:

- a written contract has been entered into with a customer for an indefinite period;
- a payment is made through the account of a person or customer participating in a transaction, which has been opened in a credit institution or the branch of a foreign credit institution registered in the Estonian commercial register or in a credit institution which has been registered or has its place of business in a contracting state of the European Economic Area or in a country where requirements equal to those provided for in this Act are in force;
- the obligated person has established by rules of internal procedure beforehand that the annual total value of performance of financial obligations arising from transactions of such type does not exceed the maximum limit of 200,000 kroons.

(5) The criteria of the low risk of money laundering or terrorist financing with regard to certain persons or transactions in the case of which simplified due diligence measures may be applied shall be established by the Minister of Finance.

### **Enhanced due diligence measures apply if:**

- (1) a person or customer participating in a transaction or official act performed in economic or professional activities has been identified and verified without being present at the same place as the person or customer;

- (2) upon identification or verification of a person suspicion arises of the truthfulness of the data or authenticity of the documents submitted or that the beneficial owner has not or that the beneficial owners have not been identified;
- (3) a person or customer participating in a transaction is politically exposed person
- (4) In the events specified in subsections (1) and (2) an obligated person shall apply at least one of the following enhanced due diligence measures:
- identification and verification of a person on the basis of additional documents, data or information, which originates from a reliable and independent source or a credit institution or the branch of a credit institution registered in the Estonian commercial register or a credit institution, which has been registered or has its place of business in a contracting state of the European Economic Area or in a country where requirements equal to this Act are in force, and if in such credit institution the person has been identified while being present at the same place as the person;
  - application of additional measures for the purpose of verifying the authenticity of documents and the data contained therein, among other things, demanding that they be notarised or officially authenticated or confirmation of the correctness of the data by the credit institution specified in clause 1), which issued the document;
  - making the first payment relating to a transaction through an account opened in the name of a person or customer participating in the transaction in a credit institution which has its place of business in a contracting state of the European Economic Area or in a country where requirements equal to those provided for in this Act are in force.
- (5) In the events specified in subsections (1) and (2) an obligated person shall apply the due diligence measures specified in clause 13 (1) 5) more frequently than usually.
- (6) An obligated person is responsible for proper application of due diligence measures.

Customer enhanced due diligence represents a set of risk-based activities, that are performed in addition to customer due diligence in order to identify beneficiary owner (BO), to verify, that a person, that has been indicated as BO is a real customer's BO Perform enhanced monitoring of customer transactions.

[EXISTING GUIDELINES TO THE BANKING INDUSTRY]

Estonian Banking Association has adopted the following non-binding guidelines:

1. **Additional Recommended Measures of EBA in order to Prevent Money Laundering in Credit Institutions.** These additional measures include more detailed instructions for banks to require additional documentation and information when opening a new account or performing transactions (2001).
2. **Additional Recommended Measures of EBA to Credit Institutions in Relations with Foreign Legal Persons to Improve Prevention of Money Laundering.** These additional measures include more detailed instructions for banks (documents (form and language) and data required upon conclusion of settlement agreements, special clauses for acceptance and treatment of the documents and additional restrictions) in relations with foreign legal persons, special attention on those, who have been founded in off-shore regions (2002).
3. **Indicators of Suspicious Transactions.** This document includes a classification of indicators upon opening of account, performing of transactions and analysis of transactions (2002). The criteria have been amended several times according to the adoption of new requirements by the regulators.
4. **Standard Information Sheet on the origin of assets of the customer** (2004).
5. **Standard Information Sheet on the information of a Estonian resident individual** while entering into a settlement contract with a bank (2003).
6. **Standard Information Sheet on the information of a Estonian non- resident individual** while entering into a settlement contract with a bank (2003)

Although the guidelines are non-compulsory, all the member banks have declared to use them as a basis while preparing their internal rules.

[GENERAL FEEDBACK (NEW MODUS OPERANDI, TRENDS, REAL CASES, etc)]

**Trends of money laundering:**

- Acquiring of assets using loan or leasing financing on basis of forged information and/or sleeping companies
- Transactions from Russia are exchanged to USD or EUR and transported back in cash
- Takeover of companies using forgery and transaction of assets using fictive bills
  
- Sleeping companies specialized on issuing fictive invoices, laundering of assets earned with tax fraud

## Top reasons for informing FIU

- One big or several smaller cash withdrawals from ATM network
- One big or several smaller cash withdrawals from branches when not fitting customers profile
- Suspicion of dummy
- One big or several smaller transfers to account
- Customer can't explain the reason for ordered services
- One extraordinary transaction not fitting customers profile

### [PURPOSES FOR WHICH THE FEEDBACK INFORMATION MAY BE USED]

The feedback from the FIU could be used in order to find latest development and methods of money laundering and terrorist financing. That would allow appropriate change settings for monitoring systems and detect possible additional money laundering and terrorist financing cases.

### [PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK STAFF IN THE EVENT OF NOTIFICATION) OF THE INSTITUTIONS OR PERSONS COVERED BY THIS DIRECTIVE ]

Credit and financial institutions and other parties subject to the Money Laundering Prevention Act, their employees and persons who have acted on their behalf are not liable for any loss suffered by the client as a result of their not executing the transaction or not executing the transaction in time following notification made to the MLIB of suspected money laundering.

No manager, employee or other person may be accused of a breach of the obligation of confidentiality, either under law or contractually, on the basis of data disclosed to the MLIB

### [CONSERVATION OF RECORDS AND DOCUMENTS]

A person shall preserve the original copies or copies of the documents, which serve as the basis for identification and verification of a person, and the documents serving as the basis for establishment of a business relationship no less than five years after termination of the business relationship.

An obligated person shall preserve the documents prepared with regard to a transaction on any data medium and the documents and data serving as the basis for the notification obligations for no less than five years after entry into the transaction or performance of the notification obligation.

A person shall preserve the documents and data specified in sections in a manner which allows for a full and immediate reply to enquiries received from the Financial Intelligence Unit or other investigative bodies or a court pursuant to legislation.

[STEPS TAKEN TO INCREASE AWARENESS OF THE PHENOMENON OF MONEY LAUNDERING (E.G.: TRAINING, INFORMATION...)]

Numerous training courses to AML specialist of covered entities including ACAMS exams.

### **Internal training of employees**

Yearly training visits of AML specialists of Estonian banks to partner Banking associations on Europe International cooperation and knowledge exchange conducted by Estonian Banking Association Estonian Banking Association has produced for banks guidelines on additional measures to combat money laundering.

Estonian Banking Association and Ministry of Finance have published 2 issues of customer booklets in Estonian, Russian and English, available in bank branches, leasing companies etc.

Communication trough media, last active period during implementation of new Money Laundering and Terrorist Financing Prevention Act.

### [ANTI-MONEY LAUNDERING /CTF LEGISLATION]

The transposition of the third directive is due in France on 31 December 2008 at the latest. Therefore all the answers below are based on the current legislation *i.e.* on the second AML directive as codified in Livre V Titre VI of the Monetary and Financial Code.

The anti-money laundering legislation is as follows:

- Monetary and Financial Code: articles L 561-1 and the following articles, and articles R562-1 and the following articles;
- Decision CNIL (body in charge of the control of the personal data protection) n° 2007-060;
- Decree n° 2007-545 of 11 April 2007 related to freezing of funds;
- Ministerial order of 21 July 2006 containing the list of equivalent countries;
- Decree n° 2006-736 of 26 July 2006;
- Act n° 2006-64 of 23 January 2006;
- Decision CNIL n° 2005-297 of 1st December 2005;
- Act n° 2004-204 of 9 March 2004;
- Act n° 2003-706 of 1st August 2003;
- Decree n° 2001-875 of 25th September 2001;
- Act n° 2001-420 of 15th May 2001;
- CRBF order n° 2002-01 of 18 April 2002;
- Instruction n° 2000-09 of 18th October 2000 of Commission Bancaire;
- Act n° 96-392 of 13th May 1996;
- CRBF order n° 91-07 of 15th February 1991;
- Decree n° 91-160 of 13th February 1991;
- Act n° 90-614 of 12th July 1990.

## [PENALTIES IN NATIONAL LAW FOR FAILURE TO RESPECT OF THE NATIONAL PROVISIONS TO THE DIRECTIVE]

Article L 562-8 of the Monetary and Financial Code provides for amounts or transactions for which the required reports have been made, proceedings on the grounds of breach of professional secrecy (articles 226-13 and 226-14 of the Penal Code) cannot be brought against the directors and employees of the financial institution or against the other persons mentioned in the legislation who made the reports in good faith.

It also specifies that no action for damages in civil proceedings can be taken, nor any professional sanction be imposed on a financial institution, its directors or employees or on any of the persons mentioned in the legislation who made the required reports in good faith.

If any loss results directly from these reports, the State assumes liability for the loss suffered. These provisions apply even if no proof is given of the criminal nature of the acts on which the report is based, and also if a court terminates proceedings or discharges or acquits the accused.

When the transaction has been executed after a report to TRACFIN that does not raise any objection from the FIU, and unless there is fraudulent collaboration with the owner of the funds or the principal of the transaction, the financial institution has no liability, and its directors or employees cannot be prosecuted on these grounds by application of articles 222-34 to 222-41 (drug trafficking), 321-1, 2, and 3 (offence of handling stolen goods or concealing objects obtained through crime) and 324-1 (offence of money laundering) of the Penal Code. The other persons subject to the suspicious transaction reporting obligation also have no liability.

In the event of a serious lack of due care or any failure in its internal control procedures, a credit institution may be subject to sanctions imposed by the Banking Commission (warning, fine, etc.). However, these are professional, not penal sanctions.

As per the new law n° 2006-64:

- The fact of the executives or agents of financial institutions or the other persons referred to in Article L. 562-1, with the exception of legal counsel and other legal professionals of the *Conseil d'Etat* and of the Court of Cassation, informing the owner of the sums or the initiator of one of the transactions referred to in Article L. 562-2 of the existence of the declaration made to TRACFIN, or divulging information concerning the likely consequences thereof shall incur a fine of €22,500.
- The fact of any executive or employee of a financial entity or person referred to in Article L. 564-1, or any person against whom a freezing or prohibition measure is applied pursuant to Chapter IV of Part VI, eluding the obligations resulting there from, or impeding implementation thereof, shall incur the penalties imposed by Article 459 of the Customs Code (five years imprisonment and fine up to the double

of the value of the infraction for the individual and five time more for a legal entity).

- When, as a result of either a serious lack of diligence or a failure in the organisation of its internal verification procedures, a financial entity or a person referred to in Article L.562-1 has failed to meet the obligations imposed on them, the authority having disciplinary powers may act automatically, as provided for in the professional or administrative rules.

## [CENTRAL AUTHORITY FOR REPORTING]

The central authority for reporting is called *Traitement du renseignement et action contre les circuits financiers clandestins* (TRACFIN) placed under the auspices of two ministers, the Minister of Economy and the Minister of Budget.

## [PERSONS RESPONSIBLE FOR REPORTING]

There is a designated correspondent in each bank or group of banks. However, any financial institution staff may report to TRACFIN in case of an exceptional situation, or in case of emergency, and as soon as possible, inform the designated correspondent who will confirm the reporting.

## [BUSINESS COVERED BY THE LEGISLATION (WHICH SPECIFIC PERSONS: NOTARIES, LAWYERS...)]

The following are subject to the suspicious transaction reporting obligation (articles L 562-1 and L 562-2 of the Monetary and Financial Code):

- Financial institutions (establishments in the banking sector, *Banque de France*, insurance companies and insurance brokers, investment companies, bureaux de change, etc.). They are also subject to other reporting obligations and vigilance obligations;
- Persons who carry out, monitor or advise on transactions relating to the purchase, sale, transfer or rental of real estate (since an Act of 1998);
- Legal representatives and directors responsible for casinos (since the Act of 15 May 2001);
- Persons who normally engage in the trading of, or organise the sale of: precious stones, precious materials, antiques and works of art (since the Act of 15 May 2001).
- Independent auditors and auditors;

- Solicitors, bailiffs, receivers, attorneys and lawyers;
- Auctioneers and voluntary companies organising public auctions.

In addition, persons other than those mentioned above who, in the performance of their profession, carry out, monitor or advise on transactions resulting in the movement of capital are obliged to report to the Public Prosecutor any transactions of which they are aware that relate to sums that they know are derived from drug trafficking or organised criminal activities (article L 561-1 of the Monetary and Financial Code).

## [PREDICATE OFFENCES COVERED]

The general offence of money laundering, created by the act n° 96-392 of 13 May 1996, establishes a general offence of money laundering and covers the proceeds of crimes and offences. However, the suspicious transaction reports that the institutions (to which the obligations apply) have to make, only relate to transactions or amounts which may be derived from drug trafficking, organised criminal activity, fraud against the European Communities' financial interests, corruption, or that which could contribute to Terrorism Financing. The scope of the offence of money laundering and the scope of the suspicious transaction report are therefore not the same.

## [IDENTIFICATION]

### **a. Definition (e.g.: PEPs, beneficial owner, thresholds...)**

As neither the directive n° 2005/60/EC nor the directive n° 2006/70/EC have been transposed, no definition of PEP is currently given by French laws. However, the French institutions are in the process of implementing the control of PEPs as per the definition of the directive.

### **b. Identification threshold amount**

Before opening an account, financial institutions must check the identity of the party to the contract based on the presentation of any written documentary evidence. They must also check the identity of occasional customers who ask them to carry out transactions over €8,000 or to hire a safe. Occasional customers are defined as persons who are neither customer of the branch they approach, or of any branch of the bank. Persons who go to a branch where they are not known, but who have an account at another branch of the same bank, are not considered as occasional customers.

**c. Identification at a distance (non face to face)**

Before opening an account, financial institutions are required to reinforce their identification measure in the case of a non-face to face opening of an account by a natural person by requesting the presentation of two identification documents instead of one.

**d. Outsourcing of identification to third parties**

N/A

**e. Means of identification**

Before opening an account, financial organisations must check the identity of their customer using documentary evidence.

- Natural persons: An official identification document with a photo of the person concerned;
- Legal persons: The original or a certified copy of any act or extract from an official commercial register showing the name, legal form and head office, together with the powers of persons acting on behalf of the company;
- Natural or legal persons acting for the account of a third person: They must ascertain the real identity of the persons on whose behalf an account is being opened or an operation is being performed when they suspect that the persons opening an account, or initiating an operation, are not acting on their own behalf. They can rely on any document which they feel appropriate.

**f. Source of information (e.g.: public register for the identification of beneficial owner)**

The French AML legislation do not impose any means for checking the identification of the beneficial owner and therefore the financial institution may use any document subject to personal data protection and banking secrecy laws.

[PRODUCTS AND TRANSACTIONS CHARACTERISED BY A HIGH/LOW RISK OF MONEY LAUNDERING]

Banks have vigilance obligations such as:

- obligation to monitor specific transactions over € 150,000 which have unusually complex conditions and do not seem to have any economic justification or lawful

purpose. Banks must ask the customer to provide information about the transaction's characteristics and record these in writing.

- Act n°. 93-122 of 29 July 1993, amending the Act of 12 July 1990.
- Suspicious transaction reports are extended to cover amounts and transactions that appear to be derived from the activities of criminal organisations.
- Act n°. 2001-420 of 15 May 2001.
- This Act imposes new obligations on financial institutions in addition to the existing suspicious transaction reporting obligation. The following must be reported automatically to TRACFIN:
  - any transaction where the identity of the principal or beneficiary remains doubtful despite the identity checks that financial institutions have to carry out;
  - any transaction involving a foundation (and in particular a trust) where the identity of the principal or beneficiaries is unknown;
  - transactions of a certain amount, carried out with certain countries or territories, whose legislation or practices are considered by the FATF as insufficient or an obstacle to combating money laundering. These reporting obligations are specified on a case-by-case basis by decree (the first decree to be adopted on the basis of this provision was decree n°2002-145 of 7 February 2002, which made it obligatory for financial institutions to report to TRACFIN any transactions carried out on behalf of a customer or a customer's principal in an amount greater than €8,000, with persons resident, registered or established in Nauru. A second decree n° 2003 – 1195 of 15 December 2003 set up the same obligations for Myanmar);
- The Act of 15 May 2001 also amended the scope of the suspicious transaction report, which now covers amounts and transactions that “may” (instead of “appear to”) be derived from drug trafficking or “organised criminal activity” (instead of “the activities of criminal organisations”). These new expressions significantly extend the scope of the suspicious transaction report insofar as:
  - with regard to the first, a report must now be filed if there is a mere doubt about the possibility of drug trafficking or organised criminal activity, even in the absence of specific or conclusive evidence;
  - with regard to the second, the aim now is for the law to take into account criminal behaviour rather than criminal structures.
- The Act n° 2004 – 130 of 11 February 2004 extends the scope of the suspicious transactions report to amount and transaction that could be derived from fraud against the European Communities' financial interests and corruption.

This Act also extends the obligation to report suspicious transactions to lawyers, notaries, and other independent legal professionals.

- The Act n° 2004 – 204 extends the scope of the suspicious transactions report to amount and transactions that could contribute to terrorism financing.
- Regulation n°. 2002-01 of 18 April 2002 relating to vigilance obligations with regard to cheques for the purpose of combating money laundering imposes specific obligations on banks with regard to cheque monitoring.

## [EXISTING GUIDELINES TO THE BANKING INDUSTRY]

The supervisor has not published new guidelines for the banking industry on this subject since its instruction n° 2000-09 of 18 October 2000.

## [GENERAL FEEDBACK (NEW MODUS OPERANDI, TRENDS, REAL CASES, etc)]

There is limited provision for feedback from TRACFIN. TRACFIN centralises the intelligence gathering and analyses the information. It forwards the information, if necessary, to the legal authorities and informs the notifying party that this has been done. It is then subject to the official secrecy covering all legal proceedings.

## [PURPOSES FOR WHICH THE FEEDBACK INFORMATION MAY BE USED]

The information passed on to TRACFIN in this connection cannot be used for any purpose other than combating the laundering of money derived from drug trafficking, organized criminal activity, fraud against the European Communities' financial interests, corruption or that which could contribute to Terrorism Financing.

## [PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK STAFF IN THE EVENT OF NOTIFICATION) OF THE INSTITUTIONS OR PERSONS COVERED BY THIS DIRECTIVE ]

Article L 562-8 of the Monetary and Financial Code provides that, for amounts or transactions for which the required reports have been made, proceedings on the grounds of breach of professional secrecy (articles 226-13 and 226-14 of the Penal Code) cannot be brought against the directors and employees of the financial institution or against the other persons mentioned in the legislation who made the reports in good faith.

It also specifies that no action for damages in civil proceedings can be taken, nor any professional sanction imposed on a financial institution, its directors or employees, or on any of the persons mentioned in the legislation who made the required reports in good faith.

If any loss results directly from these reports, the State assumes liability for the loss suffered. These provisions apply even if no proof is given of the criminal nature of the acts on which the report is based, and also if a court terminates proceedings or discharges or acquits the accused. When the transaction has been executed after a report has been made, in accordance with TRACFIN's instructions, and unless there is fraudulent collaboration with the owner of the funds or the principal of the transaction, the financial institution has no liability, and its directors or employees cannot be prosecuted on these grounds by application of articles 222-34 to 222-41 (drug trafficking), 321-1, 2, and 3 (offence of handling stolen goods or concealing objects obtained through crime) and 324-1 (offence of money laundering) of the Penal Code. The other persons subject to the suspicious transaction reporting obligation also have no liability.

In the event of a serious lack of due care or any failure in its internal control procedures, a credit institution may be subject to sanctions imposed by the Banking Commission (warning, fine, etc.). However, these are professional, not penal sanctions.

## [CONSERVATION OF RECORDS AND DOCUMENTS]

### a) *Duration*

Probative evidence is kept for 5 – 10 - 30 years (depending on the relevant statutory provisions).

### b) *Means of conservation*

Original documents are required, but in practice banks only keep cheques for large amounts. Other documents are placed on microfilm after 4 years, with insurance being taken out against the risk of losing a case or against being obliged to pay compensation for non-compliance in this area.

## [STEPS TAKEN TO INCREASE AWARENESS OF THE PHENOMENON OF MONEY LAUNDERING (E.G.: TRAINING, INFORMATION...)]

In 2003 the French Banking Federation launched a system of awareness and training with regard to combating money laundering, aimed at the entire banking profession. In 2004, 73 financial institutions and 216,000 bank employees benefited from this tool to fight against money laundering.

## GERMANY

Association of German Banks

### [ANTI-MONEY LAUNDERING /CTF LEGISLATION]

The German Money Laundering Act (*Geldwäschegesetz -GwG*) came into force on 29 November 1993. It was introduced in the course of the implementation of the first EU AML directive. The German Money Laundering Act was complemented by a new provision in the Criminal Code imposing criminal sanctions on natural persons who knowingly or grossly negligent participate in money laundering.

Since this date, there have been three major amendments: The first major amendments followed from the Act on Improving Measures to Combat Organised Crime of 4 May 1998. Further significant changes were then brought about in 2002 by the Act against Money Laundering and Terrorist Financing of 8 August 2002, which implemented, inter alia, the second EU AML directive.

The most comprehensive changes to the German legal AML framework were recently brought about by the law implementing the third EU AML directive and the directive on implementing measures, the Supplemental Money Laundering Act, which came into force on 21 August 2008. This Act effectively replaced the existing German Money Laundering Act with a completely amended version thereof and included a number of additional new provisions in the German Banking Act concerning bank specific AML obligations.

### [PENALTIES IN NATIONAL LAW FOR FAILURE TO RESPECT OF THE NATIONAL PROVISIONS TO THE DIRECTIVE]

Administrative offences are deemed to have been committed and fines may be imposed for failure to comply, or to comply correctly, with the German Money Laundering Act or AML provision of the German Banking Act.

Natural persons can also be subject to criminal sanctions (fines and/or imprisonment) in accordance with Section 261 of the Criminal Code (StGB).

### [CENTRAL AUTHORITY FOR REPORTING]

Suspicious transaction reports (STR) have to be filed with the competent prosecution authorities. As a consequence of Germany's federal structure these are the prosecution authorities of the federal states. However, a copy of each STR has to be sent to the Federal Office of Criminal Investigation (*Bundeskriminalamt/BKA*), where a Central Unit for suspicious transaction reports

(Financial Intelligence Unit - FIU) has been set up as a consequence of the 2002 amendments of the German Money Laundering Act.

## [PERSONS RESPONSIBLE FOR REPORTING]

The obligation to file an STR lies upon the entities/institutions covered by the AML obligations of the German Money Laundering Act.

## [BUSINESS COVERED BY THE LEGISLATION (WHICH SPECIFIC PERSONS: NOTARIES, LAWYERS...)]

Following the amendments the Money Laundering Act now covers:

- credit institutions, financial services institutions and financial enterprises as defined by Section 1 of the German Banking Act (i.e. providers of financial services in a broad sense); branches of foreign financial institutions are covered as well
- insurance companies which offer life insurance policies and/or accident insurance policies with premium redemption; for most of the obligations, insurance brokers are deemed to be insurance companies
- insurance intermediaries lawyers, legal advisers who are members of a chamber of lawyers, patent lawyers and notaries when they work towards the planning or execution of specific financial transactions for their clients
- qualified auditors, certified accountants, tax consultants and agents in tax matters
- real estate brokers
- gambling casinos
- bullion dealers
- auctioneers
- other natural or legal persons carrying out a business or a trade, as well as persons who administer another person's assets against payment for the fulfilment of their administrative duties; also persons acting on behalf of those enterprises.

## [PREDICATE OFFENCES COVERED]

The Money Laundering Act covers not only drug-related offences but also all serious crime pursuant to Section 261 StGB as well as all crimes related to the financing of terrorists. Serious tax-related crimes are also included.

[IDENTIFICATION]

**a. Definition (e.g.: PEPs, beneficial owner, thresholds...)**

The new German Money Laundering Act has implemented the definitions of the third EU AML directive directly or, in the case of PEP, refers to the directive on implementing measures. However, the understanding and practical implementation of these definitions will be subject to a guidance to be developed by the banking industry.

The German Money Laundering Act has implemented the general threshold of € 15.000 as regards the customer due diligence (cdd) obligations in relation to transactions outside an existing business relationship. However, the AML provisions in the German Banking Act sets out a stricter threshold of € 2.500 with regard to all currency/foreign exchange transactions. Cdd obligations are always to be attended, if there is a non-account based “cross-border money transfer”.

**b. Identification threshold amount**

See above.

**c. Identification at a distance (non face to face)**

The German Money Laundering Act contains a provision implementing Art. 13 section 2 of the third EU AML directive allowing the non face to face acceptance of customers subject to certain requirements regarding the identification of these customers.

**d. Outsourcing of identification to third parties**

In accordance with the third EU AML directive, certain institutions (i.e. other banks, insurance firms, notaries public situated in the EU or countries conforming to equivalent requirements can be relied upon for the performance of the cdd requirements. Furthermore, other third parties may be relied upon if contractual arrangements are in place covering the relevant cdd requirements. The “PostIdent”-procedure is accepted by the supervisory authority to conform to the existing legal requirements and can thus be relied upon.

**e. Means of identification**

- *Natural persons*

For the purpose of verification of the identifying principle, only qualified identity documentation conforming to the relevant requirements of the German Passport Act, such as the official identity card or passport, can be relied upon.

- *Legal persons*

Extracts from official registers (Commercial Register, association register etc.)

**f. Source of information (e.g.: public register for the identification of beneficial owner)**

Official registers can be relied upon for identification purposes as regards legal persons (see above). The most important are the commercial register, the register of association, the register of cooperatives and the land/home charge register.

## [PRODUCTS AND TRANSACTIONS CHARACTERISED BY A HIGH/LOW RISK OF MONEY LAUNDERING]

The AML provisions in the German Banking Act set out detailed requirements to be met by products which can be considered as low risk within the meaning of the directive on implementing measures. No individual class of product is named as such. In accordance with the third EU AML directive, PEP, non-face to face acceptance of customers and correspondent banking are considered as high risk.

## [EXISTING GUIDELINES TO THE BANKING INDUSTRY]

The German banking industry committee (Zentraler Kreditausschuss / ZKA) has developed first guidelines for the interpretation and implementation of the new German AML legal framework, which have been made available to the banks in December 2008.

## [GENERAL FEEDBACK (NEW MODUS OPERANDI, TRENDS, REAL CASES, etc)]

There is no general feedback obligation for the authorities receiving STR. However, the German FIU regularly issues a newsletter with information on trends and cases.

## [PURPOSES FOR WHICH THE FEEDBACK INFORMATION MAY BE USED]

The Money Laundering Act provides for the information collected to be used for prosecuting criminal offences mentioned in Section 261 StGB. Furthermore, the information provided with an STR may be used for prosecuting other serious crimes. Public prosecutors are obliged to give the information they have at their disposal to the tax authorities when information obtained in connection with criminal proceedings is believed to be valuable for an action by the tax authorities. In this case, the information may be used for tax proceedings and for the criminal prosecution of tax offences.

## [PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK STAFF IN THE EVENT OF NOTIFICATION) OF THE INSTITUTIONS OR PERSONS COVERED BY THIS DIRECTIVE ]

There are no specific provisions on the protection of employees. However, the entity or natural person filing an STR cannot be held liable for the consequences of an erroneous STR, unless the reporting entity/person has acted intentionally or grossly negligent.

## [CONSERVATION OF RECORDS AND DOCUMENTS]

### a) *Duration*

Records have to be kept for 5 years (counting from the end of the calendar year in which the customer relationship ends to which the information relates, respectively, as regards transactions outside a customer relationship, the year in which the information was obtained.

### b) *Means of conservation*

Records may be stored electronically.

## [STEPS TAKEN TO INCREASE AWARENESS OF THE PHENOMENON OF MONEY LAUNDERING (E.G.: TRAINING, INFORMATION...)]

Information about money laundering is exchanged in a contact group operated by the Ministry of the Interior. Furthermore, there are round tables with the Financial Service Authority (*Bundesanstalt für Finanzdienstleistungsaufsicht/BaFin*) and the associations of the banking industry.

The Association of German Banks keeps its members informed about legislative developments and other trends. In addition, a working group within the Association offers a forum to discuss all issues relating to money laundering. The Association regularly organises conferences/seminars.

Banks organise their own training programmes.

### [ANTI-MONEY LAUNDERING /CTF LEGISLATION]

(1) Law 3691/2008 (**Government Gazette A' 166/5.8.2008**) on prevention and suppression of money laundering and terrorist financing was adopted on 1 August 2008. It transposes the provisions of the Community Directive 2005/60/EC and Commission Directive 2006/70/EC and imposes heavy penalties, including the seizure and confiscation of property.

(2) List of laws, regulations and other AML and CTF material

#### Codes

- The Greek Criminal Code
- The Greek Criminal Procedure Code
- The Greek Civil Code

#### Laws

- Law 3601/2007 on the taking up and pursuit of the business of credit institutions, the capital adequacy of investment firms and credit institutions and other provisions [*law implementing Directives 2006/46/EC, 2006/48/EC and 2006/49/EC*]
- Law 3606/2007 on Markets and Financial Instruments [*implementing law implementing the Directive 2004/39/EC*]
- Law 3440/2005 for the protection of the capital market from insider dealing and market manipulation
- Law 3251/2004 - European Arrest Warrant
- Law 3103/2003 - Passport issuance by the Hellenic Police Authorities and other provisions
- Law 3213/2003 - Declaration and audit of the assets of members of Parliament
- Law 3148/2003 - Accounting Standardisation and Audit Committee, replacement and supplementation of the provisions on electronic money institutions, and other provisions
- Law 3126/2003 - Ministers' Criminal Responsibility
- Law 3074/2002 - Public Administration General Inspector. Upgrading the Public Administration Inspection-Audit Corps and the Inspection and Auditing Steering Body
- Law 3016/2002 - Special Issues relating to the Administration and Function of Incorporated Firms Listed in an Organised market in Greece

- Law 2802/2000 - Ratification of the Convention on the Fight Against Corruption involving Officials of the EC or Officials of the Member States of the EU
- Law 2713/1999 - Hellenic Police Internal Affairs Division
- Law 2656/1998 - Ratification of the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions
- Law 2515/1997 - Authorisation of bureaux de change
- Law 2296/95 - Control of monopolies and oligopolies and protection of free competition
- Law 2343/1995 - Reorganisation of the Services of the Ministry of Finance and other provisions
- Law 2234/1994 that amends Emergency Law 89/67- Foreign Shipping Companies
- Law 2206/1994 - Establishment, organization, operation, control of casinos and other provisions
- Law 1969/1991 - Portfolio investment companies, mutual funds, provisions for the modernisation and improvement of the capital market and other provisions
- Law 1059/1971 - Bank Secrecy Law
- Law 400/1970 - Authorisation of insurance companies and secrecy provisions

## **Regulations in relation to credit and financial institutions**

BoG Governor's Bank of Greece (Supervisory Authority for all credit institutions and some types of financial institutions such as leasing companies; factoring companies; bureaux de change; money remittance companies; credit companies; postal companies only to the extent that they provide money transfer services).

- Bank of Greece Governor's Act 2577/2006 - Framework of operational principles and criteria for the evaluation of internal control systems
  - Annex 1 - Outsourcing activities to third parties
  - Annex 2 - Operational risk management principles for information systems in FIs
  - Annex 3 - Content of an internal control system report by independent external auditors
  - **Annex 4 - Prevention of the use of the financial system for the purpose of ML and TF** (Government Gazette B' 1626/3.11.2006)<sup>2</sup>
- Bank of Greece Governor' Act No. 2541/27.2.2004 - Establishment and operation of bureaux de change in Greece by *sociétés anonymes* other than credit institutions

---

<sup>2</sup> Under review after the adoption of the Law 3691/5.8.2008.

- Bank of Greece Governor's Act 2526/2003
- Bank of Greece Statute
- Bank of Greece Governor's Act 2438/1998
- Code of Conduct for Financial Institutions
- Act of the Governor No. 2536/4.2.2004 - Requirements for granting authorisation to, and rules for the supervision of, money transfer intermediaries by the Bank of Greece (Bank of Greece Governor's Act 2536/4.2.2004)
- Article 15 of Law 2515/1997 - Bureaux de change
- Legislative Decree 1059 dated 20/23.12.1971 on bank deposit secrecy

### **Regulations in relation to securities**

**The Hellenic Capital Markets Commission (HCMC):** The HCMC is an independent supervisory body under the **Ministry of Economy and Finance**. It supervises securities and investment firms. Its main objective is to enforce capital market laws and regulations. The HCMC licenses investment services firms, investment intermediation firms and fund management companies. The HCMC then issues regulations to the extent provided for by law. It has also issued binding rules on AML matters.

- HCMC Board of Directors Decision 23/404/22.11.2006 (Government Gazette B' 1803/11.12.2006)<sup>3</sup>

### **Regulations in relation to insurance complies**

**The Insurance Supervision Commission for Private Insurance (HPISC):** According to the AML Law, the competent authority for monitoring compliance with the provisions of the law of the insurance companies, insurance intermediates and the branches established in Greece of insurance companies with head office out of Greece, is the Insurance Supervision Commission for Private Insurance (HPISC). Law 3229/2004 created the HPISC, which is under the authorisation of the Minister of Finance.

- HPISC Board of Directors Decision 109/2/12.2.2008 - Circular 8 (Government Gazette B' 516/24.3.2008)<sup>4</sup>

---

<sup>3</sup> Under review after the adoption of the Law 3691/5.8.2008.

<sup>4</sup> Under review after the adoption of the Law 3691/5.8.2008.

## [PENALTIES IN NATIONAL LAW FOR FAILURE TO RESPECT THE NATIONAL PROVISIONS OF THE DIRECTIVE]

The applicable criminal penalty in the case of natural persons is imprisonment for up to 10 years. This penalty possibly combined with any of the applicable administrative penalties. The penalty is more severe in cases where “the perpetrator exercises such activities professionally or is especially dangerous or is a recidivist.” In such cases, the penalty is imprisonment of at least ten years unless there is a case of a more severe sentence.

For legal persons, the applicable administrative penalties range from fines to exclusion from tenders, as set out below. The applicable administrative penalties for legal persons, imposed by a joint decision by the Minister of Justice and any other competent minister, as the case may be, are the following:

- temporary or permanent removal of the operating licence of the business for a period ranging from one month to two years or, if no such licence is prescribed by the law, prohibition of practice of commercial activities;
- temporary or permanent exclusion from entitlement to public benefits or aid or participation in public contract award procedures for the same period of time;
- administrative fine of EUR 30,000 to EUR 3,000,000.

Greece is implementing U.N. Security Council Resolution 1373 (2001) by several means. Law 3251/2004 introduced the criminal offence of financing of terrorism and also provided for administrative penalties to be applied against legal persons involved in terrorist offences.

## [CENTRAL AUTHORITY FOR REPORTING]

A special Commission (also called Commission of the Article 7 of the Law 3691/2008) was first established under Presidential decree N°401/10.12.96 in order to collect, assess, and investigate the information reported to it in relation to transactions suspected of being linked to money laundering. If there are reasons for believing that a transaction is suspicious, it will forward the relevant file to the public prosecutor. Where suspicions are believed to be unfounded, the cases are kept in the Commission’s archives for possible use in other domestic or international investigations.

The Commission must complete its investigations as soon as possible after the receipt of the report or other information concerning a possible breach of money laundering or terrorist financing legislation. The Commission also evaluates and investigates information on income derived from criminal activities which it receives from similar foreign organisations (FIUs), to which it provides every possible assistance.

## [PERSONS RESPONSIBLE FOR REPORTING]

Article 41 of the AML Law imposes a general requirement for Credit and Financial Institutions (CIs & FIs) to introduce internal AML controls and communication procedures to prevent transactions that could be connected with ML or TF. These internal policies also include reporting procedures. Article 44 of the AML Law sets out the obligation to designate a compliance officer.

In addition, Chapters 5 and 6 of Annex 4 of the BOG Governor's Act introduce requirements in relation to internal procedures and controls. CIs & FIs shall inform the BOG of the identity of the persons designed as AML/CTF compliance officers. The compliance officers shall assess any information that may lead to suspicion of ML or FT. The information shall be kept in a special file and if there is such a suspicion, she/he shall prepare a report and submit it to the FIU as soon as possible. If, as a result of the assessment, she/he decides not to report the information to the FIU, she/he shall fully justify this decision in the relevant file. Finally, CIs & FIs shall ensure that:

- all employees know the person to whom they must report;
- there is a clear and short channel of communication for reporting suspicious and/or unusual transactions to the AML/CTF Compliance Officer. The internal AML/CTF practice, procedures and controls shall be recorded in a manual, to be distributed to all employees; and
- there shall be a clear assignment of duties and responsibilities within the SI in order to ensure effective management of AML/CTF policies and procedures.

## [BUSINESS COVERED BY THE LEGISLATION (WHICH SPECIFIC PERSONS: NOTARIES, LAWYERS...)]

The AML and CTF Law (article 5) applies to the following persons and professions:

- a) credit institutions;
- b) financial institutions;
- c) venture capital companies;
- d) companies providing business capital;
- e) chartered accountants, audit firms, independent accountants and private auditors;
- f) tax consultants and tax consulting firms;
- g) real estate agents and related firms;

h) casino enterprises and casinos operating on ships flying the Greek flag, as well as public or private sector enterprises, organisations and other bodies that organize and/or conduct gambling and related agencies and agents;

i) auction houses;

j) dealers in high-value goods, only to the extent that payments are made in cash in an amount of EUR 15,000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked. A joint decision of the Minister of Economy & Finance and the Minister of Development shall lay down criteria for classification under this category;

k) auctioneers;

l) pawnbrokers;

m) notaries and other independent legal professionals, when they participate, whether by acting on behalf of and for their clients in any financial or real estate transaction, or by assisting in the planning and execution of transactions for the client concerning the:

- buying and selling of real property or business entities;
- managing of client money, securities or other assets;
- opening or management of bank, savings or securities accounts;
- organisation of contributions necessary for the creation, operation or management of companies;
- creation, operation or management of trusts, companies or similar structures.
- The provision of legal advice continues to be subject to professional secrecy, unless the lawyer or notary participates in money laundering or terrorist financing activities or if his legal advice is provided for the purpose of committing these offences or if he is aware that his client seeks legal advice in order to commit such offences.

n) Natural or legal persons providing services to companies and trusts (trust and company service providers) -except the persons under items j and m of this articles- which by way of business provide any of the following services to third parties:

- forming companies or other legal persons;
- acting as or arranging for another person to act as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons or arrangements;
- providing a registered office, business address, correspondence or administrative address and any other related services for a company, a partnership or any other legal person or arrangement;
- acting as or arranging for another person to act as a trustee of an express trust or a similar legal arrangement;

- acting as or arranging for another person to act as a nominee shareholder for another person other than a company listed on a regulated market, within the meaning of Article 17, paragraph 2, point a, hereof, that is subject to disclosure requirements in conformity with Community legislation or subject to equivalent international standards. A decision of the Minister of Development will specify the requirements for the incorporation, authorization, registration and the pursuit of business or profession referred to in this subparagraph, by natural or legal persons.

A joint decision of the Minister of Economy and Finance and the Minister of Justice may specify further categories of obligated persons and the corresponding competent authorities within the meaning of Article 6 hereof.

## [PREDICATE OFFENCES COVERED]

The AML and CTF Law (article 3): “Criminal activities” shall denote the commission of one or more of the following offences (hereinafter referred to as “predicate offences”):

- a. participation in an organized criminal group (Article 187 of the Penal Code);
- b. terrorist activities and terrorist financing (Article 187A of the Penal Code);
- c. passive bribery (Article 235 of the Penal Code);
- d. active bribery (Article 236 of the Penal Code);
- e. bribery of judges (Article 237 of the Penal Code);
- f. trafficking in human beings (Article 323A of the Penal Code);
- g. computer fraud (Article 386A of the Penal Code);
- h. sexual exploitation (Article 351 of the Penal Code);
- i. the offences provided for in Articles 20, 21, 22 and 23 of Law 3459/2006 re: “Codified Law on narcotic drugs” (Government Gazette 103 A);
- j. the offences provided for in Articles 15 and 17 of Law 2168/1993 re: “Weapons, ammunition, explosives etc.” (Government Gazette 147 A);
- k. the offences provided for in Articles 53, 54, 55, 61 and 63 of Law 3028/2002 re: “Protection of antiquities and cultural heritage in general” (Government Gazette 153 A);
- l. the offences provided for in Article 8, paragraphs 1 and 3, of Legislative Decree 181/1974 re: “Protection from ionised radiation” (Government Gazette 347 A);
- m. the offences provided for in Article 87, paragraphs 5, 6, 7, and 8, and Article 88 of Law 3386/2005 re: “Entry, residence and social integration of non-citizens on Greek territory” (Government Gazette 212 A);

- n. the offences provided for in the third, fourth and sixth Articles of Law 2803/2000 re: “Protection of the financial interests of the European Communities” (Government Gazette 48 A);
- o. bribery of a foreign civil servant and facilitation or concealment of the commission of such crime, as provided for in Articles 2 of Law 2656/1998 : “Ratification of the Convention on Bribery of Foreign Public Officials in international business transactions” (Government Gazette 265 A);
- p. bribery of employees of the European Communities or of the European Union Member States, as provided for: a) in Articles 2, 3, and 4 of the Treaty on Combating bribery of employees of the European Union or of European Union Member States, which was ratified by the first article of Law 2802/2000 (Government Gazette 47 A) and b) in the third and fourth article of Law 2802/2000;
- q. the offences provided for in Articles 29 and 30 of Law 3340/2005 re: “Protection of the capital market from actions by persons holding privileged information and from actions of market manipulation” (Government Gazette 112 A);
- r. any other offence punishable by deprivation of liberty for a minimum of more than six months and having generated any type of economic benefit.

[IDENTIFICATION]

**a. Definition (e.g.: PEPs, beneficial owner, thresholds...)**

**“Politically exposed persons”<sup>5</sup>**: natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates of such persons, as specified in Article 22 hereof

**“Beneficial owner”<sup>6</sup>** means the natural person(s) who ultimately owns or controls the customer and/or the natural person of whose behalf a transaction or activity is being conducted. The beneficial owner shall at least include:

- a) *in the case of corporate entities:*
  - o the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, other than a company listed in a regulated market that is subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards; a

<sup>5</sup> Law 3691/5.8.2008; article 4; par. 11

<sup>6</sup> Law 3691/5.8.2008; article 4; par. 16

percentage of 25% plus one share shall be deemed sufficient to meet this criterion;

- the natural person(s) who otherwise exercises control over the management of a legal entity;
- b) *In the case of legal entities, such as foundations, and legal arrangements, such as trusts, which administer and distribute funds:*
- where the future beneficiaries have already been determined, the natural person(s) who is the beneficiary of 25% or more of the property of a legal arrangement or entity;
  - where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;
  - the natural person(s) who exercises control over 25% or more of the property of a legal arrangement or entity.

## **b. Identification threshold amount**

Identification is obligatory where there are serious suspicions of money laundering. Identification is also required for any transaction amounting to 15.000 € or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked.. If the amount is not known at the time of transaction, the identification must be completed as soon as the amount is known.

## **c. Identification at a distance (non-face to face)**

SIs that provide their customers the possibility to carry out non-face to face transactions, notably when opening accounts (telephone banking, e-banking etc.) must adopt procedures that ensure their compliance with the requirements of the AML & CTF Law in relation to the identification procedures, where required. The above requirements on natural persons also apply to companies or organisations that request the opening of an account by mail or through the internet.

In order to minimise the risks arising out of the establishment of such a business relationship, SIs shall indicatively apply the following additional identification measures:

- obtain confirmation by a credit or financial institution operating in an EU Member State;
- demand that the first payment within the context of the business relationship be made through an account in the name of the customer kept with a credit institution operating in an EU Member State; and
- take appropriate measures to avoid establishing business relations with companies which the SI has reasonable grounds to suspect of being involved in illegal activities according to the AML/CTF legislation in force.

**d. Outsourcing of identification to third parties**

SIs may rely on intermediaries or other third parties to carry out the customer identification and verification procedure, applying the appropriate CDD, provided that the ultimate responsibility for customer identification and verification remains with the SI relying on such a third party.

SIs are obliged to *take adequate measures to satisfy themselves that copies of identification data and other relevant documentation relating to CDD requirements will be made available by the third party upon request without delay.* In addition, third parties are required to be subject to AML/CTF regulation and supervision and SIs are obliged to verify the quality of the supervisory regime.

Third countries situated “third parties” shall meet the following requirements:

- (1) be subject to mandatory professional registration, recognised by law;
- (2) apply CDD and record-keeping requirements and have their compliance supervised.

**e. Means of identification**

- **Natural Persons:** BoG Governor’s Act 2577/2006 Annex 4 has developed further guidance on customer identification especially with regard to the identification of natural persons (Chapter 1.3). Supervised institutions should require the customer to provide identification documents that are difficult to be forged or obtained illegally, regardless of the bank account or services concerned. Without prejudice to the specific information required for high-risk categories (Chapter 2 of Annex 4), the minimum particulars required and the documents verifying them are as follows:

<b>Natural Persons</b>	
<i>IDENTIFICATION PARTICULARS</i>	<i>IDENTIFICATION DOCUMENTS</i>
<ul style="list-style-type: none"> <li>• Full name and father’s name</li> <li>• ID number or passport number</li> <li>• Issuing authority</li> <li>• Customer’s signature specimen</li> </ul>	<ul style="list-style-type: none"> <li>• Identity card issued by a police authority</li> <li>• Valid passport</li> <li>• Identity card of persons serving in law enforcement agencies and the armed forces</li> </ul>
<ul style="list-style-type: none"> <li>• Current address</li> </ul>	<ul style="list-style-type: none"> <li>• Recent utility bill</li> <li>• Lease agreement certified by an internal revenue office</li> <li>• Tax clearance certificate issued by the internal revenue service</li> <li>• Valid stay permit</li> </ul>
<ul style="list-style-type: none"> <li>• Occupation and current occupational address</li> </ul>	<ul style="list-style-type: none"> <li>• Employer’s certificate</li> <li>• Tax clearance certificate issued by the internal revenue</li> </ul>

	<p>service</p> <ul style="list-style-type: none"> <li>• Copy of the last payroll slip</li> <li>• Self-employment start-up declaration</li> <li>• Occupational identity card</li> <li>• Certificate issued by a social security fund</li> </ul>
<ul style="list-style-type: none"> <li>• Taxpayer's identification number</li> </ul>	<ul style="list-style-type: none"> <li>• Tax clearance certificate issued by the internal revenue service</li> </ul>

- **Legal Persons:** BoG Governor's Act 2577/2006 Annex 4 requires that the following information be collected concerning the identification of legal entities:

<b>Legal entities</b>	
1.	<p><b>Sociétés anonymes and limited liability companies:</b> The Sociétés Anonymes &amp; Limited Liability Companies Issue of the Government Gazette where a summary of the charter of the société anonyme or limited liability company was published, including:</p> <ul style="list-style-type: none"> <li>• the name, registered office, object, number of directors (for Sociétés anonymes) and names of administrators (for limited liability companies);</li> <li>• the names and identity particulars of the company's representatives and their powers;</li> <li>• the number and date of the decision of the authority that approved the formation of the société anonyme or the registration number referred to in Article 8(1) of Law 3190/1955 "Limited Liability Companies";</li> <li>• Government Gazette issues in which any amendments to the charter in connection with the above particulars were published; and</li> <li>• the identity particulars of the legal representatives and all persons authorised to operate the company's account.</li> </ul>
2.	<p><b>Partnerships:</b></p> <ul style="list-style-type: none"> <li>• certified copy of the original partnership agreement that has been filed with the court of first instance, including any amendments thereto; and</li> <li>• the identity particulars of the legal representatives and all persons authorised to operate the company's account.</li> </ul>
3.	<p><b>Other legal entities:</b></p> <ul style="list-style-type: none"> <li>• their establishing documents, certified by a public authority; and</li> <li>• the identity particulars of the legal representatives and all persons authorised to operate the company's account.</li> </ul>

**f. Source of information (e.g.: public register for the identification of beneficial owner)**

See the means of identification above

## [PRODUCTS AND TRANSACTIONS CHARACTERISED BY A HIGH/LOW RISK OF MONEY LAUNDERING]

Table III of BOG Governor's Act 2577/2006 Annex 4 provides an indicative list of transactions that should be examined with special attention:

- Customers who provide insufficient or suspicious identification;
- Wire transfers;
- Activities inconsistent with the customer's business;
- Cash transactions;
- Use of safe deposit boxes;
- Loans;
- Purchases and/or sales of securities;
- Changes in bank-to-bank transactions;
- Suspicious behaviour of employees;
- Money laundering through international trade.

By 31 May 2007, supervised institutions are required to adopt adequate IT systems and effective procedures for the ongoing monitoring of accounts and transactions, in order to detect, monitor and assess high-risk transactions and customers. The BOG Governor's Act Annex 4 sets out further indicative measures for implementing a risk management system:

- Assessment of the risk facing the financial institution (transactions structure, review of basic clientele, regions of activity, procedures, products, distribution networks and organisation);
- Recording and identification of customer, product and transaction-specific risks, using the expertise and techniques applied in the banking sector. The expertise required is obtained and updated on the basis, *inter alia*, of the international typology of suspicious events (including the relevant typology which the Bank of Greece Department for the Supervision of Credit and Financial Institutions requires on a minimum basis and periodically communicates to financial institutions), assessment of press articles, analysis of suspicious events that the institution becomes aware of and exchange of experience with the AML/CTF Compliance Officers;
- Development, through electronic data processing, of adequate parameters based on the results of the financial institution's risk analysis;
- Review and further development of preventive measures, taking into account the results of risk analysis.

## [EXISTING GUIDELINES TO THE BANKING INDUSTRY]

The BOG issued a list of examples of potentially suspicious transactions (BoG Governor's Act 2577/2006 Annex 4 – Table III unusual or suspicious transactions) and the HCMC included a similar but much shorter list in the Board of Directors Decision 23/404/22.11.2006.

BOG Governor's Act 2577/2006 Annex 4, Chapter 2 contains guidelines that require **enhanced due diligence/monitoring** for certain types of transactions and customers. These include:

- Non-residents' accounts;
- Accounts of politically exposed persons from third countries (i.e. non-EU);
- Accounts of companies with bearer shares;
- Accounts of offshore etc. companies;
- Accounts of non-profit organisations;
- Portfolio Management Accounts of important clients;
- Non-face to face transactions;
- Cross-border correspondent banking relationships with respondent institutions from third countries (i.e. non-EU);
- Countries which do not comply adequately with the FATF recommendations.

Specific additional customer identification and record-keeping requirements apply to each of these categories.

Supervised Institutions are required to scrutinise high-risk accounts, according to the inherent risk, in order to decide whether or not to maintain them. The employee in charge of monitoring the account is required to prepare a brief report stating the results of the review and send it to the AML/CTF Compliance Officer. The AML/CTF Compliance Officer is, in turn, required to submit a report to the financial institution's management for approval.

In practice, the banking industry has already developed its own categories of client/account where higher levels of due diligence are performed, often for reasons wider than AML/TF (e.g. fraud, credit risk etc.).

## [GENERAL FEEDBACK (NEW MODUS OPERANDI, TRENDS, REAL CASES, etc.)]

The Greek FIU prepares an annual report which includes general feedback, statistics on the number of disclosures (with appropriate breakdowns), and on the results of the disclosures. However, there is no information on current ML techniques, methods and trends (typologies) and no sanitised examples of actual ML cases.

There is no specific or case-by-case feedback other than acknowledgment of receipt when the STR is delivered to the FIU headquarters – any follow-up is on an *ad hoc* basis.

## [PURPOSES FOR WHICH THE FEEDBACK INFORMATION MAY BE USED]

The feedback information may be used to assist reporting entities in improving the quality of STRs submitted, and to help identify new areas where suspicion might arise.

## [PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK STAFF IN THE EVENT OF NOTIFICATION) OF THE INSTITUTIONS OR PERSONS COVERED BY THIS DIRECTIVE ]

Article 32 of the AML/CTF Law provide SIs and their directors, officers and employees protection when reporting STRs, and states that the provision of information to the FIU and other law enforcement and judicial authorities does not constitute a breach of contract and cannot give rise to any liability when done in good faith. This protection seems to be available even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

Article 31 criminalises disclosure of the fact that an STR or related information have been submitted or requested or that a money laundering or terrorist financing investigation is being carried out. Breach of this provision can result in three months imprisonment and a fine. This provision applies to SIs and their directors and employees as well as employees of competent authorities and the Commission of the Article 7 (the FIU).

According to Article 30, a joint decision of the Minister of Economy and Finance and the Minister of Justice may specify measures to protect the obligated persons' employees and obligated natural persons reporting, either internally or externally to the Commission (FIU) or the Public Prosecutor, suspected cases of committing or attempting to commit the offences set out in Article 2, form threats or hostile acts.

## [CONSERVATION OF RECORDS AND DOCUMENTS]

Credit and Financial Institutions (CIs & FIs) are obliged to keep for a period of at least five years - unless a longer period is provided for in a legal provision - after the business relationship with the customers has ended, (as far as agreements are concerned), and for a period of at least five years following the last transaction, (as far as transactions are concerned), the data relevant to the abovementioned agreements and transactions, such as legalization documents, copies of documents (on the basis of which the verification of the customer's identity took place), and transaction evidence.

Within the framework of complying with the requirement of the previous paragraph, the CIs & FIs keep, at the very least, the following data:

- the customer's identity, including his full name, address, phone number, profession, office address, tax reference number and signature sample;
- the number of the provision of investment services accounts;

- the identity of the beneficial owners;
- the identity of the persons authorised to act on behalf of the customer;
- data relating to the size and the transactions carried out;
- the connected bank accounts of the customer;
- the source of the funds;
- the type and the amount of the transaction's currency;
- the way in which the funds have been deposited or withdrawn, that is cash, checks, transfers etc.;
- the identity of the person who gave an order for carrying-out of the transaction;
- the purpose of the funds;
- the type of instructions given by the customer.

CIs & FIs shall have information systems or procedures that will enable them to respond completely and promptly to a question submitted by the Commission (FIU), as to whether they have or had during the period of the last five years a business relationship with particular natural persons, or legal entities, and as to the type of such business relationship.

CIs & FIs shall keep the data for a period of at least five years, either in hard copies or in electronic files, and the files which prove their compliance with the obligations provided for in this decision. Record keeping may be also carried out in electronic form, on the condition that the relevant information systems follow controlled access procedures, user ID and date.

[STEPS TAKEN TO INCREASE AWARENESS OF THE PHENOMENON OF MONEY LAUNDERING (E.G.: TRAINING, INFORMATION...)]

BoG Governor's Act 2577/2006 Annex 4 (Chapter 7) contains specific provisions for training of staff on AML/CTF issues. Credit and Financial institutions must develop employee training (including web training) programmes. In the context of these programmes:

- employees shall be informed on the legislation and the legal obligations of the staff, as well as the procedures adopted, including customer identification, record keeping and internal reporting procedures;
- the duration and subject of training programmes shall be tailored to each staff category (newly-hired, front office, compliance, customer recruitment staff); and
- training programmes shall be repeated regularly, in order to ensure that the staff knows their duties and obligations and are kept abreast of developments.

The Hellenic Bank Association (via the Hellenic Banking Institute) offers training to compliance officers and senior staff of banks, and to branch network staff.

The Hellenic Bank Association has produced a useful leaflet aimed at informing consumers (physical persons) about why banks are obliged to request identity information. The information leaflet has been printed by HBAs member banks and is available for the customers through their branch network.

INFORMATION REQUIRED ACCORDING TO THE LAW	DOCUMENTS WHICH CAN VERIFY YOUR PERSONAL INFORMATION (as the case may be)		Have you introduced yourselves?
Identification Information	<ul style="list-style-type: none"> <li>■ Identity Card</li> <li>■ Valid Passport</li> <li>■ ID card for persons serving in Law Enforcement and Armed Forces</li> </ul>	<p>You have to produce original copies of the above documents, while banks have to keep copies thereof.</p> <p>The information that your bank will request may vary depending on your transaction type and amount. <b>Additional information may thus be required</b>, included VAT returns, invoices, bills of lading, ownership titles, lease or sale agreements and/or other documentation.</p>	
Current Home Address	<ul style="list-style-type: none"> <li>■ Recent utility bill</li> <li>■ Lease agreement submitted to a Tax Office</li> <li>■ Itemized Tax Payment Statement</li> <li>■ Valid Residence Permit</li> </ul>	<p><b>When acting on behalf of another person</b>, in addition to providing your personal identification documents, you will be required to produce evidence of the third natural or legal person on behalf of which you are acting. Banks are obliged to demand and verify such information as well, according to the law.</p>	
Current Profession and Professional Address	<ul style="list-style-type: none"> <li>■ Employer's certificate</li> <li>■ Itemized Tax Payment Statement</li> <li>■ Copy of last salary statement</li> <li>■ Incorporation Statement</li> <li>■ Professional Identification Card</li> <li>■ Insurance Organization Contribution Payment Invoice</li> </ul>		<p>If not... ...do it now</p>
Tax Registration Number (AFM)	<ul style="list-style-type: none"> <li>■ Itemized Tax Payment Statement</li> </ul>	<p>Let us thank you for your co-operation and the time you spent reading this document.</p> <p>HELLENIC BANK ASSOCIATION www.hba.gr</p>	

## HUNGARY

Hungarian Banking Association

### [ANTI-MONEY LAUNDERING /CTF LEGISLATION]

Act CXXXVI of 2007 on the Prevention and Combating of Money Laundering and Terrorist Financing

### [PENALTIES IN NATIONAL LAW FOR FAILURE TO RESPECT OF THE NATIONAL PROVISIONS TO THE DIRECTIVE]

In this case the Hungarian Financial Supervisory Authority (HFSA) shall take the following measures consistent with the weight of the infringement:

- a) call upon the service provider to take the measures necessary for compliance with the provisions of this Act, and to eliminate the discrepancies;
- b) advise the service provider:
  - to ensure the participation of their relevant employees (managers) carrying out the activities listed under Subsection (1) of Section 1 in special ongoing training programs, or to hire employees (managers) with the appropriate professional skills required for those activities;
  - to draw up the by-laws within the prescribed deadline, or to adapt it according to specific criteria;
- c) issue a warning to the service provider;
- d) order the service provider to cease the unlawful conduct;
- e) in addition to or independent of the measures specified in Paragraphs a)-d), impose a fine of minimum two hundred thousand and maximum five million forints

### [CENTRAL AUTHORITY FOR REPORTING]

National Financial Intelligence Unit within the Hungarian Customs and Finance Guard

### [PERSONS RESPONSIBLE FOR REPORTING]

The bank shall, depending on the structure of the organization, designate one or more persons (hereinafter referred to as "liaison officer") to forward without delay the reports received from the employees of the bank to the national financial intelligence unit. Banks are required to notify the national financial intelligence unit concerning the appointment of the liaison officer, including

the name and the position of such officer, and any subsequent changes therein, within five working days of the date of appointment or the effective date of the change.

## [BUSINESS COVERED BY THE LEGISLATION (WHICH SPECIFIC PERSONS: NOTARIES, LAWYERS...)]

- a) financial services auxiliary to financial services;
- b) investment services, auxiliary to investment services investment fund management services;
- c) insurance services, insurance agency or occupational retirement provision;
- d) commodity exchange services;
- e) postal financial intermediation services, postal money transfers, accepting and delivering domestic and international postal money orders;
- f) real estate agency or brokering and any related services;
- g) auditing services;
- h) accountancy (bookkeeping), tax consulting services or tax advisory activities
- i) the operation of a casino or electronic casino;
- j) the trading in precious metals or articles made of precious metals;
- k) the trading in goods, involving a cash payment in the amount of three million six hundred thousand forints or more;
- l) voluntary mutual insurance fund services;
- m) the provision of legal counsel or notary services.

## [PREDICATE OFFENCES COVERED]

All criminal activities committed by others, that is punishable by imprisonment (all crime approach).

## [IDENTIFICATION]

### **a. Definition (e.g.: PEPs, beneficial owner, thresholds...)**

**PEP:** means natural persons residing in another Member State or in a third country who are or have been entrusted with prominent public functions within one year before the implementation of customer due diligence measures, and immediate family members, or persons known to be close associates, of such persons.

- a) heads of State, heads of government, ministers and deputy or assistant ministers;
- b) members of parliaments;

- c) members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal;
- d) the head of the court of auditors, members of courts of auditors or of the boards of central banks;
- e) ambassadors, chargés d'affaires and high-ranking officers in the armed forces;
- f) members of the administrative, management or supervisory bodies of State-owned enterprises.

**'beneficial owner' means:**

- a. the natural person who owns or controls at least twenty-five per cent of the shares or voting rights in a legal person or business association lacking the legal status of a legal person, if that legal person or business association lacking the legal status of a legal person is not listed on a regulated market and is subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards;
- b. the natural person who has a dominant influence in a legal person or business association lacking the legal status of a legal person as defined in Subsection (2) of Section 685/B of Act IV of 1959 on the Civil Code of the Republic of Hungary (hereinafter referred to as "Civil Code");
- c. the natural person on whose behalf a transaction is carried out; and
- d. in the case of foundations:
  - 1. where the future beneficiaries have already been determined, the natural person(s) who is the beneficiary of twenty-five per cent or more of the property of the foundation;
  - 2. where the individuals that benefit from the foundation have yet to be determined, the class of natural persons in whose main interest the foundation is set up or operates or
  - 3. the natural person(s) who exercises control in the management of the foundation or exercises control over twenty-five per cent of the property of a foundation, or who is authorized to represent the foundation;

**b. Identification threshold amount**

- million HUF or more
- In the case of exchanging money: 500,000 HUF

**c. Identification at a distance (non face to face)**

No

**d. Outsourcing of identification to third parties**

Yes, if it is carried out by a financial service provider operating in Hungary, in the EU or in a third country having an AML legislation equal to the EU standards.

**e. Means of identification**

Recording in writing of the data of the customer who is present as a general rule.

**f. Source of information (e.g.: public register for the identification of beneficial owner)**

Yes

[PRODUCTS AND TRANSACTIONS CHARACTERISED BY A HIGH/LOW RISK OF MONEY LAUNDERING]

High risk:

- if the customer is not present,
- PEPs,
- exchange of money up to 500,00 HUF or more,

Low risk if the customer is:

- a financial service provider from the EU,
- listed companies,
- FSAs,
- central government bodies, local authorities,
- EU institutions,
- life insurances under 260,000 HUF etc.

[EXISTING GUIDELINES TO THE BANKING INDUSTRY]

Model Rules issued by the HFSA, self- regulation: Recommendation 5/2008 of the Hungarian Banking Association.

[GENERAL FEEDBACK (NEW MODUS OPERANDI, TRENDS, REAL CASES, etc)]

Yes, every 6 months from the Hungarian FIU.

## [PURPOSES FOR WHICH THE FEEDBACK INFORMATION MAY BE USED]

To be sure that the FIU received the STR.

Remark: as of the 15th December 2008 STRs are to be submitted via a secured internet page.

## [PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK STAFF IN THE EVENT OF NOTIFICATION) OF THE INSTITUTIONS OR PERSONS COVERED BY THIS DIRECTIVE ]

In practice yes, but not in the law.

## [CONSERVATION OF RECORDS AND DOCUMENTS]

8 years

## [STEPS TAKEN TO INCREASE AWARENESS OF THE PHENOMENON OF MONEY LAUNDERING (E.G.: TRAINING, INFORMATION...)]

Regular trainings, exchange of best practices, common seminars with the FIU.

## IRELAND

Irish Banking Federation

### [ANTI-MONEY LAUNDERING /CTF LEGISLATION]

The main provisions in Irish law relating to Money Laundering/Terrorist Financing are set out in Section 31 of the **Criminal Justice Act 1994**, (as amended by Section 21 of the **Criminal Justice (Theft and Fraud Offences) Act 2001**), Sections 32 and 57 of the Criminal Justice Act 1994, and Section 23 of the Criminal Justice (Theft and Fraud Offences) Act 2001. The **Criminal Justice (Terrorist Offences) Act 2005** amended Sections 32 and 57 of the Criminal Justice Act 1994 to include the offence of financing terrorism.

The legislation is supplemented by Guidance for various sectors (including credit and financial institutions) which may be relied upon by a designated body or individual when demonstrating compliance with the legislative provisions.

The 3<sup>rd</sup> AML Directive has not yet been implemented in Ireland although a draft General Scheme of the new AML Bill was published in February 2008 for consultation purposes. The new legislation which is expected shortly will repeal, replace and consolidate existing legislation.

The Guidance is also under review and the redrafting process is at an advanced stage. The new Guidance will have a core section with applicability to all sectors and sectoral guidance for specific sectors.

**Please note: All answers below are based on existing legislation.**

### [PENALTIES IN NATIONAL LAW FOR FAILURE TO RESPECT OF THE NATIONAL PROVISIONS TO THE DIRECTIVE]

The Criminal Justice Act 1994 sets out the various offences which are deemed to be felonies. A person found guilty of an offence can be faced with a fine or imprisonment for up to 14 years.

If the Financial Regulator suspects a breach of Irish AML/CFT law its only possible course of action would be to submit an STR to the FIU. It is also possible that in certain cases the facts giving rise to a breach of the legislation and/or guidance notes may also constitute a breach of requirements which are the subject of administrative sanctions.

### [CENTRAL AUTHORITY FOR REPORTING]

The Financial Intelligence Unit (FIU) was formed in 1995 following the enactment of the Criminal Justice Act (1994) that required designated institutions to report STRs. The FIU is part of the Garda Síochána (Police) and operates autonomously within the Garda Bureau of Fraud Investigation (GBFI) as a law enforcement style FIU that is able to exchange information within and outside the Garda through police information exchange channels.

Since 2003 STRs are also sent to the Revenue Commissioners.

## [PERSONS RESPONSIBLE FOR REPORTING]

Designated bodies and their employees are responsible for reporting.

The guidance notes require each designated body to appoint an MLRO and the MLRO has responsibility for deciding whether the information contained in reports received from staff should be reported to the Gardaí and the Revenue Commissioners.

The guidance notes specify that an employee is in compliance with their obligation to report a suspicious transaction if they have reported their suspicion in accordance with the internal procedure established within their designated body.

Also, the Financial Regulator is obliged to report to the Gardaí and Revenue Commissioners any information relevant to that body that leads it to suspect that a criminal offence may have been committed by a supervised entity.

## [BUSINESS COVERED BY THE LEGISLATION (WHICH SPECIFIC PERSONS: NOTARIES, LAWYERS...)]

The current legislation covers the following entities/activities;

- Banks, building societies, money brokers, trustee savings banks, life assurance providers, persons providing a service in financial futures and options exchanges, An Post (national post service), Credit Unions, persons providing a service in relation to buying and selling stocks, shares and other securities and persons providing foreign currency exchange services
- Accountants (other than an accountant who provides a service in his or her capacity as an accountant to a person who employs him or her under a contract of service)
- Auctioneers and estate agents
- Auditors and tax advisers
- solicitors where the activity consists of the provision of assistance in;
  - the planning or execution of transactions for clients concerning the buying or selling of land or business entities
  - managing of client money, securities or other assets
  - opening or management of bank, savings or securities accounts
  - organisation of contributions necessary for the creation, operation or management of companies

- creation, operation or management of trusts, companies or similar structures
- acting on behalf of and for a client in any financial transaction or transaction relating to land
- the provision of services to a person in connection with the purchase or sale of land where payment for the land concerned is in cash and is not less than €13,000
- the provision of [investment business services](#) or [investment advice](#),
- the carrying out of trustee or custodian duties for a [collective investment scheme](#)
- the provision of money remittance services
- Activities of administration companies consisting of the provision of services to [collective investment schemes](#)
- Activities of dealers in high value goods, including precious stones, precious metals and works of art where payment for the goods concerned is in cash and is not less than €15,000
- Activity of operating a casino

## [PREDICATE OFFENCES COVERED]

The money laundering offence relates to “property” which represents the proceeds of criminal conduct. “Criminal conduct” is conduct which constitutes an indictable offence if committed within the State. Therefore, predicate offences include all indictable offences. Under Irish law, crimes are classified as either summary offences or indictable offences. Summary offences are offences of a minor nature and are those which are tried before a judge without a jury. Indictable offences are offences which may (at accused’s election) or must be tried on indictment before a judge and jury.

## [IDENTIFICATION]

The focus of current legislation is on KYC principles. Guidance provides details on customer identification but it does not address 3<sup>rd</sup> Directive elements such as PEPs.

The Guidance does provide detail on how to establish identity and the type of documentation/methods that should be used in verifying identity.

### **a. Definition (beneficial owner)**

The requirement to identify beneficial ownership is contained in s. 32 (5) of the CJA (1994), which requires that where a designated body proposes to provide a service for a person to whom it knows or has reason to believe to be acting for a third party, it shall take “reasonable measures” to establish the identity of the third party.

**b. Identification threshold amount**

Identification must be established on entering into a business relationship or opening an account, or in respect of individual transactions amounting to €13,000 or more or, in respect of a series of transactions, which are or appear to be linked and which amount in aggregate to €13,000 or more or in any other case (irrespective of the amount) where money laundering is suspected regardless of the amount.

**c. Identification at a distance (non face to face)**

The Guidance provides information on the types of evidence that should constitute satisfactory confirmation of identity on a non-face to face basis.

**d. Outsourcing of identification to third parties**

The Guidance states that in the case of a single transaction to be effected by a financial institution for a person introduced to it by another designated body, it is regarded as reasonable for the financial institution, in establishing identity, to rely on the written assurance of the designated body or corresponding body that it has established the person's identity and holds evidence of that identity and will provide copies of such evidence if requested to do so. The name and address of the customer must also be provided in writing by the introducing body. If the person being introduced forms any continuing relationship with the financial institution, then the financial institution concerned must itself obtain separate evidence of identity.

**e. Means of identification**

The CJA (1994) does not specify what constitutes adequate evidence of identity but the Guidance provides goes into some detail about the different types of identification that could be used in different scenarios.

**f. Source of information (e.g.: public register for the identification of beneficial owner)**

No public register exists for the identification of beneficial owner per se but the Companies Registration Office (CRO) may be consulted for a fee. The CRO is the central repository of public statutory information on Irish companies and business names.

[PRODUCTS AND TRANSACTIONS CHARACTERISED BY A HIGH/LOW RISK OF MONEY LAUNDERING]

The Guidance does make some distinctions as to products and transactions which are of a higher/lower risk but the risk based approach as a concept is not currently reflected in legislation or guidance.

## [EXISTING GUIDELINES TO THE BANKING INDUSTRY]

Sectoral guidance notes complement the AML obligations under the CJA (1994) and provide additional more detailed information for the banking sector on how to implement AML/CFT measures. The guidance notes are issued by the Money Laundering Steering Committee (MLSC), which is made up of different government agencies and private sector bodies. The guidance notes provide an explanation on the requirements of the CJA (1994) and its amendments; provide a steer on internal controls, policies and procedures as well as dealing with many aspects of CDD, record keeping, STR reporting and education and training procedures. Guidance to financial institutions has also been provided in relation to Terrorist Financing after the enactment of the Criminal Justice (Terrorist Offences) Act (2005). While not legally binding, the Guidance Notes establish the requisite standards of regulatory compliance and may be taken into account by a court in assessing whether an institution has fulfilled its statutory obligations.

## [GENERAL FEEDBACK (NEW MODUS OPERANDI, TRENDS, REAL CASES, etc)]

The FIU and Revenue Commissioners provide regular feedback to Industry based on STR's received and they highlight trends and new developments. The MLSC also provides a forum through which practical experiences may be shared. Irish Banking Federation runs several Committees and Working Groups on AML which meet regularly to discuss new developments.

## [PURPOSES FOR WHICH THE FEEDBACK INFORMATION MAY BE USED]

It increases the designated bodies understanding of their role in the detection, investigation and prosecution of those that are involved in money laundering. It aids in the development of training and assists in system enhancement which will ultimately improve detection of money laundering.

## [PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK STAFF IN THE EVENT OF NOTIFICATION) OF THE INSTITUTIONS OR PERSONS COVERED BY THIS DIRECTIVE ]

The protection of employees of designated bodies is ensured by s.57 (7) of the CJA (1994), stating that pursuant to a suspicious transaction disclosure made in good faith the person making the disclosure should not incur a liability of any kind for breaching any statutory or other restriction upon the disclosure of information.

Section 58 (2) of the CJA (1994) states that where a report has been made, a person who knowing or suspecting that such a report has been made, makes any disclosure which is likely to prejudice any investigation arising from the report shall be guilty of a "tipping off" offence.

## [CONSERVATION OF RECORDS AND DOCUMENTS]

Section 32, (9) of the CJA (1994) requires that designated bodies retain:

- a) a copy of all materials used to identify a customer or prospective customer
- b) the original documents or copies admissible in legal proceedings relating to any transaction.

Documents must be retained for a period of 5 years after the business relationship has ended or the last transaction has been executed.

## [STEPS TAKEN TO INCREASE AWARENESS OF THE PHENOMENON OF MONEY LAUNDERING (E.G.: TRAINING, INFORMATION...)]

Statutory obligations exist regarding staff training in s.32 (9B) of the CJA (1994) as amended.

The guidance notes set out the details and appropriate measures to be taken by designated bodies to fulfil the education and training requirements of the legislation. The Guidance also includes a section on internal controls, policies and procedures. This requires that institutions have adequate arrangements and procedures in place to provide continuing training programmes for employees.

### [ANTI-MONEY LAUNDERING /CTF LEGISLATION]

The Third Directive as well as Commission Directive 2006/70/EC have been implemented in Italy through Legislative Decree no. 231 of 21 November 2007, (entered into force on 29 December 2007 and, for art. 49 – on cash, checks and passbooks - on 30 April 2008). Legislative Decree no. 231 of 21 November 2007 entered into force on 29 December 2007 and repealed and replaced, in almost its entirety, the prior law contained in Law Decree no. 143 of 3 May 1991, converted with amendments by Law no. 197 of 5 July 1991 as well as Legislative Decree no. 56 of 20 February 2004, and related implementing ministerial regulations.

Legislative Decree no. 231/ 2007 sets forth that the measure enacted to implement the repealed and replaced legislation continue to be applied, insofar as they are compatible with the new legislation, until the date the implementing measures of the new decree enter into force. With specific reference to intermediaries, the prior legislation, for which a residual application has been envisaged until the adoption of the new secondary legislation, consists of:

- Ministerial Decree no. 142 of 3 February 2006 that regulates anti-money laundering obligations imposed on financial intermediaries in implementing Legislative Decree no. 56 of 20 February 2004;
- Italian Exchange Office and Financial Intelligence Unit Measure of 24 February 2006 containing the applicable instructions for intermediaries on the requirements of identification, registration and conservation of information for purposes of preventing and combating money laundering by using the financial system;
- Operational guidelines for reporting suspicious transactions (so-called “rulebook”) issued by the Bank of Italy on 12 January 2001;
- Italian Exchange Office and Financial Intelligence Unit circular dated 22 August 1997, modified by circular of 27 February 2006, sets out instructions for reporting transactions by financial and credit intermediaries.

The Ministry of Economics and Finance, by a measure published on 19 December 2007, identified provisions deemed immediately repealed or incompatible, as well as the provisions of those measures that continue to be applied. Specifically it appears that:

- For the identification and registration requirements, the amount Euro 12,500 is replaced by the new limit of Euro 15,000;

- The new definitions contained in Legislative Decree no. 231/2007 and, specifically, the concept of fractioned and related transactions, as well as that of money laundering and financing terrorism replace those prior;
- All obligations concerning customer due diligence requirements and of beneficial owners are immediately applicable: accordingly the obligations contemplated by Ministerial Decree no. 142 of 3 February 2006 and Italian Exchange Office and Financial Intelligence Unit Measure of 24 February 2006 must be integrated with the new obligations set out in Legislative Decree no. 231/2007;
- The new “risk-based approach” principle is immediately applicable;
- The indicators of anomaly contained in the Bank of Italy rulebook will continue to be applied vis-à-vis reporting suspicious transactions.

And Legislative Decree no. 109 of 22 June 2007. This legislation repeals and replaces the prior Italian legislation contained in Law Decree no. 143 of 3 May 1991, converted with amendments by Law no. 197 of 5 July 1991, as well as Legislative Decree no. 56 of 20 February 2004, and related implementing regulations.

On the basis of Law Decree no. 112 of 25 June 2008, (converted by Law no. 133 of 6 August 2008) the limit of 12,500 Euro was re-imposed for cash transfers, checks and bearer savings book.

[PENALTIES IN NATIONAL LAW FOR FAILURE TO RESPECT OF THE NATIONAL PROVISIONS TO THE DIRECTIVE]

Anti-money laundering laws provide for criminal and administrative sanctions. The table below illustrates the most important sanctions.

	<b>Criminal sanctions</b>	<b>Administrative sanctions</b>
<b>Due diligence requirements</b>	<p>Failure to fulfil the provisions related to customer due diligence concerning the identification requirement is punishable by a fine in an amount from Euro 2,000 to Euro 13,000.</p> <p>The person carrying out the transaction who omits providing the particulars of</p>	<p>With respect to the failure to follow the instructions issued by the Supervisory Authority on customer due diligence, an administrative fine shall be imposed in an amount from Euro 10,000 to Euro 200,000.</p>

	<p>the party on whose behalf he/she is carrying out the transaction or provides false information, is punishable by imprisonment from 6 months to 1 year and a fine in an amount from Euro 500 to Euro 5,000.</p> <p>In case the identification requirement was fulfilled by using fraudulent means, which obstructed identification of the party who carried out the transaction, the above fine is doubled.</p> <p>If person carrying out the transaction does not provide information on the purpose and intended nature of the business relationship or provides false information, he/she is punishable by imprisonment from 6 months to 3 years with a fine in an amount from Euro 5,000 to Euro 50,000.</p>	
<p><b>Registration requirements</b></p>	<p>Anyone, under a duty, who omits registering the information, or registers it late or makes an incomplete registration, is punishable by a fine in an amount from Euro 2,600 to Euro 13,000. In case the registration requirement was fulfilled by using fraudulent means, which obstructed identification of the party</p>	<p>With respect to the failure to comply with the instructions issued by the Supervisory Authority on the registration requirement, an administrative fine shall be imposed in an amount from Euro 10,000 to Euro 200,000.</p> <p>Failure to set up a single</p>

	<p>who carried out the transaction, the above fine is doubled.</p>	<p>computerized data base (Archivio Unico Informatico) is punishable by an administrative sanction in an amount from Euro 50,000 to Euro 500,000. In more serious cases, in consideration of the gravity of the violation inferred from the circumstances of same and the violation's duration, in addition to the fine, the infringer shall be ordered to publish a summary of the relevant penalty order in at least two national newspapers, including in one that is a financial newspaper, at his/her own expense.</p>
<p><b>Requirement to report suspicious transactions</b></p>	<p>Anyone, under a duty, who violates the prohibition on disclosing a reporting of suspicious transactions, or the prohibition on disclosing feedback from the Financial Information Unit to the intermediary, is punishable by imprisonment from 6 months to 1 year with a fine in an amount from Euro 5,000 to Euro 50,000.</p> <p>Members of the board of auditors, advisory board, management control committee, and supervisory board under Legislative Decree no. 231/2001 and all other parties entrusted</p>	<p>Failure to report suspicious transactions is punishable by an administrative fine in an amount from 1% to 40 % of the unreported transaction's amount. In more serious cases, in consideration of the gravity of the violation inferred from the circumstances of same and the unreported transaction's amount, in addition to the fine, the infringer shall be ordered to publish a summary of the relevant penalty order in at least two national newspapers, including in one that is a financial</p>

	<p>with management control, no matter their job title, who fail to communicate to the business owner or the company's legal representative or one of his/her appointed managers of violations of the provisions on reporting suspicious transactions, are punishable by imprisonment up to 1 year and a fine in an amount from Euro 100 to Euro 1,000.</p>	<p>newspaper, at his/her own expense. It must be noted that the Supervisory Authorities shall inform the Financial Information Unit of possible cases of non-compliance of the requirement to report suspicious transactions that they detect during their monitoring activities over intermediaries.</p> <p>Failure to comply with an order to suspend a transaction issued by the Financial Information Unit, unless it constitutes a crime, is punishable by an administrative fine in an amount from Euro 5,000 to Euro 200,000.</p>
<p><b>Limitation on the use of cash and bearer securities</b></p>		<p>With respect to violations of the prohibition to transfer cash or bearer bank and postal passbooks for amounts equal to or exceeding Euro 12,500, a fine shall be applied in an amount from 1 % to 40 % of the transferred amount.</p> <p>With respect to violations on the provisions requiring that bank and postal cheques issued for an amount equal to or exceeding Euro 12,500 must indicate the name or company name of the payee and bear the non-</p>

		<p>transferability clause, a fine shall be applied in an amount from 1 % to 40 % of the transferred amount.</p> <p>In case of violations of the provisions requiring that bank and postal cheques made payable to the drawer can only be endorsed for cashing at a bank or Poste Italiane s.p.a., a fine shall be applied in an amount from 1 % to 40 % of the transferred amount.</p> <p>In case of violations of the provisions requiring that bank drafts, postal orders and promissory notes must indicate the name or company name of the payee and bear the non-transferability clause, a fine shall be applied in an amount from 1 % to 40 % of the transferred amount.</p> <p>With respect to violations on the provisions requiring that the balance in bearer bank and postal passbooks cannot be equal to or exceeding Euro 12,500, a fine shall be applied in an amount from 20% to 40 % of the balance.</p> <p>In case of violations of the rules on settling the balance in bearer bank</p>
--	--	---

		<p>and postal passbooks when the balance is equal to or exceeds Euro 12,500, i.e., to reduce the balance to below the limit, which must be completed by 30 June 2009, a fine shall be applied from 10% to 20 % of the bearer passbook balance.</p> <p>Violating the provision requiring that in cases of transferring bearer bank and postal passbooks, the transferor must communicate to the bank or the Poste italiane s.p.a. within 30 days, the specifications of the transferee as well as details on the transfer, will result in a fine from 10% to 20% of the bearer passbook balance</p> <p>In case of violations of the rules on limits imposed on individuals providing services for remuneration, a fine shall be applied in an amount from 20% to 40 % of the transferred amount.</p> <p>With respect to violations of the prohibition to open anonymous accounts or passbooks or those fictitiously registered, a fine shall be imposed in an amount from 20% to 40% of the balance.</p>
--	--	---

		<p>With respect to violations of the prohibition to use in any way anonymous accounts or passbooks, or those fictitiously registered, opened abroad, a fine shall be imposed in an amount from 10% to 40% of the balance.</p> <p>With respect to violations of the duty to communicate to the Ministry of Economics and Finance within thirty days of the violation being discovered by the intermediary in relation to the limitations on the use of cash and bearer securities, or anonymous accounts and passbooks or those fictitiously registered, a fine shall be imposed in an amount from 3% to 30% of the amount of the transaction, of the passbook balance or account balance.</p>
--	--	---

[CENTRAL AUTHORITY FOR REPORTING]

Starting from 1 January 2008, a financial information unit ( “Financial Information Unit“) was established within the structure of the Bank of Italy. It is entrusted with receiving [information] from the responsible parties, making requests from same, analyzing and communicating to the competent authorities’ information concerning cases of money laundering or terrorist financing. Previously, the duties of the Financial Information Unit were carried out by the UIC (Italian Exchange Office and Financial Intelligence Unit).

## [PERSONS RESPONSIBLE FOR REPORTING]

A person is appointed in each bank and banking group who is responsible for anti-money laundering; he/she must assess and forward reports of suspicious transactions to the Financial Information Unit. Banks operating in Italy must set up a single computerized data base at each bank (art. 37 of Legislative Decree no. No. 231/2007), where transactions are recorded as well as bank-customer relations and services; transactions are recorded if they are equal to or exceed Euro 15,000 Euro. Accordingly, a person is appointed to maintain the database.

## [BUSINESS COVERED BY THE LEGISLATION (WHICH SPECIFIC PERSONS: NOTARIES, LAWYERS...)]

Legislative Decree no. 231/2007 applies to professionals, auditors and others as persons, in addition to banks and other intermediaries.

### Professionals:

- certified accountants, accountants and qualified accountants
- notaries
- lawyers
- managers and administrators of companies and trusts

### Auditors:

- auditing firms
- individuals enrolled with the register of auditors

### Other parties that carry out:

- debt collection
- custody and transport of cash or securities
- management of casinos
- offers through the internet and through other on-line games, betting or contests with cash prizes
- real-estate agency

## [PREDICATE OFFENCES COVERED]

For purposes of Legislative Decree no. 231/2007, “money laundering” is:

- a) the conversion or transfer of property, carried out with the knowledge that it derives from criminal activity or from actively participating in criminal activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity in evading the legal consequences of his action;
- b) the concealment or disguise of the true nature, source, location, disposition, movement or rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an active participation in such activity;
- c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an active participation in such activity;
- d) participation in one of the activities above, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of such actions.

The Italian Penal Code's definition (art. 648-bis) is different and does not cover cases of self-laundering.

"Financing terrorism" means any activity aimed at, through any means, raising, hoarding, brokering, storing, safe-keeping or disbursing funds or financial resources, no matter the manner, intended to be used, all or in part, to carry out one or more terrorist acts as contemplated by the penal code, and therefore regardless if the funds and financial resources are actually used to commit the above crimes.

[IDENTIFICATION]

## **Customer due diligence**

### *1. Knowledge about your client.*

The new legislation requires that knowledge of one's client is not merely formal or just limited to extracting information from identification documents, but rather more substantive and includes information related to the purposes and nature of the intermediary-client relationship.

### *2. When to apply the customer due diligence measures.*

Intermediaries, even through distribution network operators, must fulfil the customer due diligence measures, when, in the course of their activity they:

- establish a business relationship with the client;
- carry out occasional transactions on the instructions of clients requiring the transferring or handling of payment means in an amount equal to or exceeding Euro 15,000,

regardless of the fact that that it was carried out in one or several transactions appearing to be fractioned and related;

- a suspicion exists as to money laundering or financing terrorism regardless of any applicable derogation, limit or exemption;
- doubts exist as to the truthfulness or adequacy of the information previously obtained to identify the client.

Customer due diligence requirements must be met, moreover, in cases in which banks, electronic money institutions or Poste Italiane s.p.a. act as a go-between or are part of the cash or bearer securities transfer, for whatever reason, between the various entities, of amounts exceeding or equal to Euro 15,000. Financial brokers must comply with customer due diligence measures also for transactions under Euro 15,000.

### *3. The content of the customer due diligence measures.*

With respect to the content of the customer due diligence measures, intermediaries, even through distribution network operators, must:

- a. identify the client and verify such identity on the basis of documents, data or information obtained from an independent and trustworthy source;
- b. identify any beneficial owner and verify such identity;
- c. acquire information on the nature and purpose of the business relationship;
- d. perform constant monitoring during the course of the relationship.

Clients also have duties to fulfil under anti-money laundering legislation. In particular, clients must furnish, under penalty of law, all the necessary and updated information to allow the intermediary to fulfil the customer due diligence measures.

In order to identify a beneficial owner, clients must provide in writing, under penalty of law, updated and necessary information of which they have knowledge.

### *4. Manners to meet the customer due diligence requirements.*

The specific manners to fulfil the customer due diligence requirements are defined and set out in detail in the anti-money laundering operational procedures adopted by the single intermediaries, a procedure that distribution network operators must have complete knowledge of and which they must apply continuously. There are, moreover, general conditions to fulfil and consequently these must be fulfilled by all intermediaries and distribution network operators.

Specifically, identifying and verifying such identity of clients and beneficial owners must be carried out with the client present and by using current identification documents before initiating business relations or effecting transactions. In case the client is a company or an entity, actual power to represent must be verified and all information must be obtained to identify and verify the identity of the appointed representative authorized to order transactions to be carried out.

The personal information to acquire is name, last name, place and date of birth, address, tax code and the details of the identification document or if the party is not an individual, the company name, registered office and tax code or, for legal entities, the VAT number. For clients on whose behalf contact was made by financial advisors, insurance agents or brokers, credit brokers or financial brokers, the intermediary may proceed with the identification by acquiring from same all the necessary financial information even without the client being present.

Identifying and verifying the identity of beneficial owners must be carried out at the same time as identifying the client. Intermediaries, based on how much risk is involved, must prepare adequate measures aimed at understanding the ownership and control structure of the client. Specifically, intermediaries can decide to utilize public registers or lists containing information on beneficial owners, to request their clients for information, or acquire information from other sources. The constant monitoring during the business relationship is carried out by analyzing concluded transactions during the course of the relationship, in order to verify that such transactions are compatible with the knowledge the intermediary has of his/her client, the client's business activities and the client's risk profile, with respect to the origins of the funds, and by updating the documents and information held by the intermediary.

Customer due diligence requirements are so fundamental that, in case intermediaries cannot comply with them, a duty of abstention is imposed. Specifically, when they are unable to identify clients, beneficial owners or obtain information on the purpose and nature of the business relationship, intermediaries cannot initiate business relations nor carry out transactions, or must put an end to business relations underway and evaluate whether to report the suspicious transaction to the Financial Information Unit.

*5. Manners to meet the customer due diligence requirements through third parties (remote identification).*

In order to avoid repeating customer due diligence procedures, an intermediary may trust the procedures carried out by third parties. Specifically, client identification by financial intermediaries can occur, even without the client, through acquiring a valid certificate issued by one of the following entities with whom the client has a relationship and for which he/she has already been identified in person:

- a. financial intermediaries and in particular banks, Poste italiane S.p.A., electronic money institutions, security brokerage firms, management companies, investment firms, life insurance companies operating in Italy, money brokers, companies performing payment collection services, financial intermediaries enrolled in a special register pursuant to art. 107 of the Consolidated Banking Law, financial intermediaries enrolled in a general register pursuant to art. 106 of the Consolidated Banking Law, Italian branches of the entities indicated above having headquarters abroad as well as Italian branches of harmonized management companies and investment firms and Cassa depositi e prestiti S.p.A.;
- b. credit and financial institutions of Member States;

- c. banks having their registered and administrative offices in non-EU countries provided the country belongs to the FATF and Italian bank branches in those countries and States belonging to FATF.

In this case the certification must be able to prove the identity between the person to be identified and the person holding the account or having business relations with the certifying intermediary, as well as the accuracy of the information communicated from a distance. The certification can take the form of a wire transfer from the account for which the client was identified in person, that contains the code issued to the client by the intermediary, which must identify the client.

## 6. The so-called “risk-based approach”.

The risks of money laundering and terrorist financing are not always the same and can vary greatly depending on the client, on the transaction and on the business relationship in question. Consequently, the customer due diligence requirements must be appropriate and commensurate with the risk of money laundering and financing terrorism (c.d. “risk-based approach”).

Without prejudice to the autonomy and responsibility of each intermediary in adopting appropriate procedures to identify clients, as well as the obligation to be consistent with the instructions adopted from the Supervisory Authority, there are certain general principles identified in the regulations in order to give an insight to the so-called “risk-based approach”. Specifically, with reference to clients, in order to identify the risk of money laundering and terrorist financing, the following must be considered:

- the legal nature;
- the primary activity carried out;
- the behaviour during the completion of the transaction or when the business relation began;
- the geographic area of residence or client’s office or counterparty’s.

With reference to the transaction or business relationship, the risk-based approach entails placing particular attention on:

- the type of operation or business relationship;
- the manner to carry out a transaction or the business relationship;
- amount;
- frequency of the transactions and the duration of the business relationship;
- reasonableness of the transaction or the business relationship with respect to the client’s business;

- geographic area of the product's destination that is the subject matter of the transaction or business relationship.

Based on the risk-based approach, the new legislation provides that:

- in cases of low risk of money laundering or terrorist financing, intermediaries may apply simplified customer due diligence procedures;
- in cases of high risk of money laundering or terrorist financing, intermediaries must apply enhanced customer due diligence procedures.

A politically exposed person is a citizen of another Member State or third country that holds or has held an important public office, and includes even immediate family members or associates with whom they have notoriously close ties.

In relation to transactions and business relationships with politically exposed persons, intermediaries must:

- a. establish adequate procedures based on risk, to determine if the client is a politically exposed person;
- b. obtain the authorization of the general manager, or another officer holding an equivalent position, prior to initiating a business relationship with the client;
- c. adopt every necessary measure to establish the source of the wealth and source of the funds that are involved in the business relationship or transactions;
- d. conduct enhanced on-going monitoring of the business relationship.

## [PRODUCTS AND TRANSACTIONS CHARACTERISED BY A HIGH/LOW RISK OF MONEY LAUNDERING]

### **Simplified customer due diligence procedure**

The so-called "risk-based approach" provides that, without prejudice to the need to assess clients, there exist cases in which it is possible to apply the "simplified customer due diligence procedure", due to the low risk of money laundering. The application of the simplified customer due diligence procedure may be justified from the qualification of the relevant client or the characteristics of the project subject matter of the transaction.

For example, the simplified customer due diligence procedure applies when the client is a bank or securities brokerage firm or management company. Therefore, identification and verification is not required if the client is an office of the public administration.

The simplified customer due diligence procedure applies, moreover in cases of life insurance policies whose annual premium does not exceed 1,000 Euro, or, in case of electronic money, if

the device cannot be recharged and the maximum amount stored in the device is no more than 150 Euro.

### **Enhanced customer due diligence procedure**

If there is a high risk of money laundering or terrorist financing, then particularly rigorous customer identification and verification procedures are required. (“Enhanced customer due diligence procedure”).

The procedure adopted by single intermediaries shall identify cases in which, in relation to the activity carried out by the specific intermediary, it is opportune to apply the enhanced customer due diligence procedure.

Without prejudice to the autonomy and responsibility of each intermediary to identify cases of high risk of money laundering and terrorist financing, there are certain cases presumed to be high risk. Specifically, intermediaries must apply enhanced customer due diligence procedures:

- if the client is not physically present;
- in case of cross-frontier correspondent banking relationships with credit institutions from third countries;
- in relation to transactions and business relationships with a politically exposed person;
- in relation to products or transaction aimed at boosting anonymity.

When the client is not physically present, intermediaries, in order to compensate for higher risks, must apply one or more of the following measures:

- ascertain the identity of the client through documents, data or additional information;
- adopt supplementary measures to verify or certify documents supplied or requiring confirmatory certification by a credit or financial institution covered by the anti-money laundering directive 2005/60/EC;
- ensure that the first payment of the operations is carried out through an account opened in the customer's name with a credit institution.

### [EXISTING GUIDELINES TO THE BANKING INDUSTRY]

The due diligence and registration requirements are useful to fulfil intermediaries' obligation to report suspicious transactions. With reference to those obligations, in order to help identify suspicious transactions, on the suggestion of the Financial Information Unit, indicators of anomaly have been issued. They are periodically updated by measures of the Bank of Italy and addressed to financial intermediaries and other parties carrying out financial services. While awaiting the issue of new indicators of anomaly, the criteria contained in the operational guidelines to report suspicious transactions (so-called “rulebook”) issued by the Bank of Italy on 12 January 2001 are applied.

Another tool of notable importance and help to intermediaries is the computerized GIANOS (GeneratoreIndiciAnomaliaOperazioniSospette) procedure, which allows identifying anomalies in transactions and behaviours of clients by using algorithms. A report of suspicious transactions does not constitute a criminal complaint but rather a report to investigate which, in turn, could ascertain criminal misconduct.

Parties responsible for reporting suspicious transactions are financial intermediaries (banks, securities brokerage firms, *Poste Italiane s.p.a*, trust companies, insurance companies, etc.), financial advisors, brokers, credit brokers, insurance intermediaries and financial brokers as well as professionals, notaries and lawyers, auditors and other parties, including, for example, those who collect debt, custody and transport of cash, public administration offices, management companies of regulated markets, casinos and real-estate agents.

With respect to the previous legislation, the objective scope of application of the reporting requirements has been broadened. This broadening is connected to, on the one hand, the new definition of “money laundering”, that is wider than the definition set out in the penal code; on the other hand, to imposing reporting requirements of suspicious transactions to cases of financing terrorism.

The obligation to forward a report of a suspicious transaction to the Financial Information Unit arises when an intermediary has knowledge of, suspects or has reason to believe that a transaction in progress, completed or attempted is for money laundering or terrorist financing purposes. This obligation arises, therefore, when an intermediary has knowledge (“*knows*”), has suspicions (“*suspects*”) or a suspicion may be inferred (“*reasonable basis to suspect*”) that a transaction is underway, completed or attempted for money laundering or terrorist financing purposes.

## [GENERAL FEEDBACK (NEW MODUS OPERANDI, TRENDS, REAL CASES, etc)]

Reports of suspicious transactions are made by intermediaries to the Financial Information Unit promptly, where possible prior to the transaction and as soon as the intermediary has suspicions. The head of personnel, the office or other operational and organizational units of the intermediary which is entrusted with the administration and management of client relationships has the duty to promptly report the suspicion to the owner of the business or to the legal representative or one of its appointed managers. Distribution network operators, as they are in direct contact with clients, are the first parties who must evaluate whether any anomalies exist in relation to transactions ordered by clients. In this assessment, distribution network operators must carefully weigh their knowledge of the client against the indicators of anomaly present in the transaction.

Financial advisors, financial brokers and credit brokers fulfil reporting requirements by forwarding a report of a suspicious transaction to the owner of the business or to the legal representative or to one of the appointed managers of the intermediary.

The owner of the business or the legal representative or one of the appointed managers (so-called “officer of anti-money laundering”) examines the reports they receive and, in case they are grounded, keeping in mind all the information in his/her possession including from the single computerized data base, they forward it to the Financial Information Unit without naming the person who made the report.

The Financial Information Unit, in relation to the reports received, must investigate by taking into account the data and information asked and received by reporting parties, information from the register on accounts and deposits and tax registry, and the information acquired by the Financial Information Unit during their analysis and examination.

If they find the report ungrounded, the Financial Information Unit will file it away but keep a record of it for a ten-year period.

In cases in which the report has merit, the Financial Information Unit promptly forwards the reports, together with a technical report, to the Anti-Mafia Investigation Unit and the *Guardia di Finanza* [Italian Finance Police], which, in turn, inform the Anti-Mafia Public Prosecutor if connected to organized crime.

Forwarding the report to the investigating bodies or the filing of the report are communicated to the reporting intermediary directly by the Financial Information Unit, unless it would harm the investigation (so-called “**feedback**”).

## [PURPOSES FOR WHICH THE FEEDBACK INFORMATION MAY BE USED]

Reports of suspicious activities, requests for investigations, as well as an exchange of information pertaining to reported suspicious transactions, between the Financial Information Unit, the *Guardia di Finanza*, Anti-Mafia Investigation Unit and the supervisory authorities, by electronic means, must be able to guarantee that only the addressed parties will receive it and that the integrity of the information has not been compromised.

## [PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK STAFF IN THE EVENT OF NOTIFICATION) OF THE INSTITUTIONS OR PERSONS COVERED BY THIS DIRECTIVE ]

Intermediaries shall adopt appropriate measures to ensure the identity of the person reporting the transaction remains confidential. Any documents containing information on this person must remain under the direct safe keeping of the owner of the business or the legal representative or one of its appointed managers.

It is important to remember that reports of suspicious transactions are forwarded by the intermediary to the Financial Information Unit without the name of the reporting party.

The Financial Information Unit, the *Guardia di Finanza* and the Anti-Mafia Investigation Unit may request the intermediary for additional information in order to analyze and examine the report without having to directly request the reporting party.

In case of a complaint or a report in accordance with arts. 331 and 347 of the Code of Criminal Procedure, the identity of the individual who made the report, even if known, is not mentioned.

The identity of the individual may only be revealed when a court, by reasoned order, deems it indispensable to ascertain the crimes, subject matter of the proceeding. In case of seizure of documents and information, the necessary measures to guarantee confidentiality of the identity of the reporting party shall be adopted.

Legislative Decree no. 231/2007 provides that the Financial Information Unit, the *Guardia di Finanza* and the Anti-Mafia Investigation Unit, after consultation with the Committee for Financial Security of the Ministry of Economics and Finance, adopt, even on the basis of memoranda of understanding, adequate measures to ensure the utmost confidentiality of the identity of reporting parties (art. 45, para. 5).

## **Prohibition of disclosure**

Parties responsible for reporting suspicious transactions or anyone having knowledge thereto are forbidden to communicate the existence of a report. Specifically, parties responsible for reporting cannot inform the person of interest or a third party of the report, pending investigation or a potential investigation on money laundering and terrorist financing. This prohibition does not prevent intermediaries belonging to the same group from communicating it amongst themselves.

The feedback at the outcome of the investigation communicated by the Financial Information Unit to the intermediary is subject to the same prohibition of disclosure vis-à-vis clients or third parties.

## [CONSERVATION OF RECORDS AND DOCUMENTS]

Intermediaries are obliged to conserve documents and register the information they acquire during the customer due diligence.

Specifically, intermediaries must conserve:

- (i) copies or references to documents requested from the client during the due diligence, for a period of ten years from the end of the business relationship;

- (ii) written documents and registrations (consisting of the original documents and copies having the same legal effect) pertaining to transactions and business relations, for a period of ten years from the execution of the transaction or the end of the business relationship.

Intermediaries must register the following information:

- (i) with respect to business relationships, the date the relationship commenced, the personal information of the client together with the general information of the person authorized to act on behalf of the person having the business relationship and the code of the relationship where applicable;
- (ii) with respect to transactions in an amount equal to or exceeding Euro 15,000, even for transactions which appear to be fractioned or related, the reason, amount, type of transaction, payment means and the personal information of the person carrying out the transaction as well as on whose behalf it is being carried out. In regards to the prior legislation that contemplated a limit of Euro 12,500, the new legislation contemplates that the registration requirement applies to transactions in an amount equal to or exceeding Euro 15,000.

The above information must be:

- conserved for **ten years**;
- promptly registered **within 30 days** after the conclusion of the transaction or the start, modification or end of the business relationship.

In cases that the intermediary receives information to be registered from a financial advisor, financial broker, credit broker or anyone else acting on behalf of the intermediary, the term of thirty days to register starts to run from the intermediary receiving the information. Any financial advisor, financial broker, credit broker or anyone else acting on behalf of the intermediary is obliged to, in turn, forward such information to the intermediary within thirty days.

## **Fractioned transactions – Related transactions**

For “**fractioned transactions**” we mean a transaction that is considered one transaction from an economic perspective with a value equal to or exceeding the limit of Euro 15,000, carried out through several operations, each under the limit, carried out at different times but within a limited time frame, set at seven days, provided the requisites exist. (ABI, by circular dated 17 April 2008 sets a limit of Euro 5,000 or more for registering fractioned operations in the single computerized database).

The new legislation added, in addition to the concept of fractioned transactions, the concept of related transactions. It is opportune to clarify the differences between fractioned and related transactions.

For “**related transaction**” we mean transactions that, even if not executed pursuant to the same contract, are connected by the person executing it, their objective and for their intended purposes.

Fractioned signifies financial flows characterized by multiple movements within a limited time (7 days) and united for the purpose of carrying out the obligations under one linked contract.

Related signifies instead financial flows characterized by multiple movements for the purpose of carrying out the obligations under multiple linked contracts, being part of a complex financial plan with one objective. In defining related transactions one disregards, therefore, the time frame during which the movements took place and one scrutinizes the objective or any other element connecting the transactions.

### **Aggregate data**

Intermediaries must forward to the Financial Information Unit, on a monthly basis, aggregate data concerning their operations, in order to allow an analysis of potential cases of money laundering or terrorist financing in certain areas. The Financial Information Unit identifies the type of data to forward according to a risk-based approach and defines the methods by which to send and aggregate the data, also by direct access to the single computerized data base.

[STEPS TAKEN TO INCREASE AWARENESS OF THE PHENOMENON OF MONEY LAUNDERING (E.G.: TRAINING, INFORMATION...)]

ABI, in terms of informing and training intermediaries, carries out intensive programmes, among which:

- High level inter-company seminars such as those carried out in March and July 2008;
- In house training, already carried out approximately 40 times for a total of 1385 employees;
- Web based course, with legislation and practical examples;
- Formative instructions to be used by bank employees.

Moreover ABI has, for some time, been committed to joint training with the Superior Council of Judges on issues of interest to judges and other investigation authorities that address banking activities.

#### [ANTI-MONEY LAUNDERING /CTF LEGISLATION]

The AML/CTF legislation in Latvia is regulated by more than 30 various legal acts. The main of which are the following:

- *The Law on the Prevention of Laundering the Proceeds from Criminal Activity and of Terrorist Financing, enacted on 17<sup>th</sup> of July, 2008, entered into force on 13<sup>th</sup> of August, 2008, thus fully implementing European Parliament and Council directives 2005/60/EC and 2006/70/EC .*
- *Provisions of Cabinet of Ministers No. 1071 “Provisions on the List of Indicators of Unusual Transactions and the Reporting Procedure regarding Unusual and Suspicious transactions” adopted on 22<sup>nd</sup> of December, 2008.*
- *Provisions of Cabinet of Ministers No. 966 “Provisions on Third Countries which imposes requirements equivalent to those of the European Union regulatory provisions with respect to the prevention of money laundering and of terrorist financing”, adopted on 25<sup>th</sup> of November, 2008.*
- *Regulations of the Financial and Capital Market Commission No. 125, “Regulations on Customer Enhanced Due Diligence” adopted on 27<sup>h</sup> of August, 2008*
- *Regulations of the Financial and Capital Market Commission No. 63, “Regulations for creation of an Internal Control System” adopted on 2<sup>nd</sup> of May, 2007*

#### [PENALTIES IN NATIONAL LAW FOR FAILURE TO RESPECT THE NATIONAL PROVISIONS TO THE DIRECTIVE]

The Financial and Capital Market Commission (FCMC) is entitled to implement one or several of the following measures: warning, specify restrictions, partially or fully suspend the provision of financial services, stop activities or impose fine up to 100,000 lats.

The applicable sentence for terrorism or terrorist financing is life imprisonment or deprivation of liberty for a term of not less than eight and not exceeding twenty years, with confiscation of property.

For a person who commits laundering of criminally acquired financial resources or other property, the applicable sentence is deprivation of liberty for a term of not less than three and not exceeding twelve years, with confiscation of property.

## [CENTRAL AUTHORITY FOR REPORTING]

The Latvian FIU – the Office for Prevention of Laundering of Proceeds Derived from Criminal Activity (Control Service for short) was established on 1 June 1998 and is a member of the Egmont Group. It is a State body, which operates under the monitoring of the Prosecutor's Office of Latvia Republic.

## [PERSONS RESPONSIBLE FOR REPORTING]

A legal person subject to Law on the Prevention of Laundering the Proceeds from Criminal Activity and of Terrorist Financing shall appoint a structural unit of one or several employees to be entitled to take decisions and be directly responsible for compliance with this Law. In addition to the general requirements, credit and financial institutions, excluding capital companies that buy and sell cash foreign currency, shall appoint a board member who shall be responsible for the prevention of money laundering and of terrorist financing in the respective credit or financial institution.

## [BUSINESS COVERED BY THE LEGISLATION (WHICH SPECIFIC PERSONS: NOTARIES, LAWYERS...)]

- Credit institutions;
- Financial institutions;
- Tax advisors, external accountants, sworn auditors in commercial companies of sworn auditors,
- Sworn notaries, sworn advocates, other independent legal professionals when they act in the name and for the benefit of their customers to assist in the planning and execution of a transaction, to participate in any transaction or to perform other professional activities related to transactions for the benefit of their customer in the following cases:
  - a. buying or selling of real estate, shares in the capital of a commercial company;
  - b. managing a customer's money, financial instruments, and other fund,;
  - c. opening or managing all kinds of accounts with credit institutions or financial institutions,
  - d. creating, managing or ensuring the operation of legal arrangements, making investments necessary for creating, managing or ensuring the operation of legal arrangements;
- Legal arrangement and company service providers;
- Persons acting in the capacity of agents or intermediaries in real estate;

- Organisers of lotteries and gambling;
- Persons providing money collection services;
- Other legal or natural persons involved in trading real estate, transport vehicles, items of culture, precious metals, precious stones and articles thereof or other goods, acting as intermediaries in the said transactions or providers of services, where the payment is made in cash in lats or another currency in the amount equivalent to or exceeding €15 000 at the exchange rate set by the Bank of Latvia on the transaction day, whether the transaction is executed in a single operation or several linked operations.

## [PREDICATE OFFENCES COVERED]

In accordance with AML/CTF Law the proceeds shall be recognised as derived from criminal activity when a person, directly or indirectly, acquires ownership or possession of them as a result of a criminal offence or in other cases specified by the Criminal Procedure Law.

The money laundering shall mean:

- Converting the proceeds from criminal activity into other valuables, changing their location or ownership;
- Concealing or disguising the true nature, source, location, disposition, movement or ownership of the proceeds from criminal activity;
- Acquiring the proceeds from criminal activity for ownership, possession or use knowing, at the time of acquiring such rights that the proceeds were derived from criminal activity;
- Participating in any of the activities mentioned above.
- Terrorist financing shall mean the activities as defined by the Criminal Law.

## [IDENTIFICATION]

### a. Definition (e.g.: PEPs, beneficial owner, thresholds...)

**Beneficial owner** – a natural person:

- Who owns or directly or indirectly controls at least 25% of the share capital or voting rights of a merchant or exercises other control over the merchant's operation,
- Who, directly or indirectly, is entitled to the property or exercises a direct or an indirect control over at least 25% of a legal arrangement other than a merchant. In the case of a foundation, a beneficial owner shall be a person or a group of persons for whose benefit the foundation has been set up. In the case of political parties, societies, and cooperative societies, a beneficial owner shall be the respective political party, society or cooperative society,
- For whose benefit or in whose interest a business relationship is established,

- For whose benefit or in whose interest a separate transaction is made without establishing a business relationship in the meaning of Law on the Prevention of Laundering the Proceeds from Criminal Activity and of Terrorist Financing;

**Politically exposed person (PEP)** - a natural person who:

- Is entrusted with one of the following prominent public functions in another member state or a third country: the head of the state, a member of the parliament, the head of the government, a minister, a deputy minister or an assistant minister, a state secretary, a judge of the supreme court, a judge of the constitutional court, a board or a council member of the court of auditors, a member of the council or of the board of a central bank, an ambassador, a chargé d'affaires, a high-ranking officer of the armed forces, a member of the council or of the board of a state-owned capital company, as well as a person who has resigned from the position of a prominent public function within one year;
- Is a parent, a spouse and a person equivalent to a spouse, a child, his/her spouse or a person equivalent to a spouse of the persons referred to in Law on the Prevention of Laundering the Proceeds from Criminal Activity and of Terrorist Financing hereof. A person shall be treated as equivalent to a spouse provided that the laws of the respective country contain a provision for such status;
- Is publicly known to have a business relationship with any person referred to in Law on the Prevention of Laundering the Proceeds from Criminal Activity and of Terrorist Financing hereof or a joint ownership with such person of the share capital in a commercial company, and a natural person that is a sole owner of a legal arrangement that is known to be established for the benefit de facto of any person referred to in Law on the Prevention of Laundering the Proceeds from Criminal Activity and of Terrorist Financing hereof.

## **b. Identification threshold amount**

The subject of the Law shall identify a customer before establishing a business relationship regardless of threshold amount. The subject of the Law shall also identify a customer before each occasional transaction when:

- Not establishing the business relationship the amount of a transaction or the total amount of several apparently linked transactions is equivalent to €15 000 or more;
- A transaction corresponds to at least one of the indicators in the list of unusual transactions or gives rise to a suspicion of money laundering, terrorist financing or an attempt thereof;
- There are doubts about the veracity of the previously obtained identification data.

**c. Identification at a distance (non- face to face)**

Where at inception of a business relationship a customer has not been identified by a person subject to the Law, its employee or authorised person, the person subject to the Law shall take any of the following steps:

- Obtain additional documents or information evidencing the customer's identity;
- Perform additional verification or certification of submitted documents or obtain a statement of a credit institution or a financial institution registered in another member state to the effect that the customer has a business relationship with that credit institution or financial institution;
- Ensure that the first payment in the course of the business relationship is carried out through an account opened in the customer's name with a credit institution to which the requirements of the Law or of the EU legislative provisions on the prevention of money laundering and of terrorist financing apply;
- Require that the customer is present when executing the first transaction.

**d. Outsourcing of identification to third parties**

A person subject to the Law shall be entitled to recognize and accept the results of the customer identification and customer due diligence performed by credit institutions and financial institutions other than capital companies that buy and sell cash foreign currency, and providers of money transmission and remittance services in a member state and a third country, provided that the requirements in respect of the prevention of money laundering and of terrorist financing as enforced in these countries, are equivalent to those of the Law.

Reliance of a person subject to the Law on the results of customer identification and customer due diligence shall be without prejudice to the duty to monitor the customer's business relationship on a continuing basis.

**e. Means of identification**

Natural persons shall be identified by verifying their identity on the basis of a personal identification document in which the following information is provided:

- Regarding a resident: the name, the surname, the personal identity number;
- Regarding a non-resident: the name, the surname, the date of birth, the number of the personal identification document and the date of issue, the issuing country and the authority which issued the document.

Natural persons, non-residents, who have personally appeared before the persons subject to this Law in Latvia shall be identified only by a valid document for immigration into Latvia.

Legal persons shall be identified by requesting that they:

- Produce documents giving evidence of their establishment or legal registration;
- Notify the registered office address of the customer;
- Identify the persons entitled to represent them in the relationship with the person subject to this Law; a document giving evidence of the rights of those persons to represent the legal person or a copy such document shall be obtained.

A person subject to the Law shall be entitled to identify a legal person by obtaining the above information from a publicly available source that is reliable and independent.

**f. Source of information (e.g.: public register for the identification of beneficial owner)**

In order to fulfil the duties as set out in the Law, credit institutions and insurance merchants that provide life insurance shall be entitled to request and, free of charge, receive information on a customer, its beneficial owners and representatives, counterparties to transactions and their beneficial owners, and also on the persons who have expressed willingness to start a business relationship with the credit institution or the insurance merchant, their beneficial owners and representatives, on the spouses of those persons and the first degree relatives from the following:

- The Register of Enterprises of the Republic of Latvia;
- The State Social Insurance Agency;
- The Invalid Documents Register;
- The Penal Register;
- The State Unified Computerised Land Register;
- The State Register of Vehicles;
- The Population Register.

[PRODUCTS AND TRANSACTIONS CHARACTERISED BY A HIGH/LOW RISK OF MONEY LAUNDERING]

Customer enhanced due diligence represents a set of risk-based activities, that are performed in addition to customer due diligence in order to

- Identify beneficiary owner (BO), to verify, that a person, that has been indicated as BO is a real customer's BO
- Perform enhanced monitoring of customer transactions.

A person subject to the Law shall perform enhanced customer due diligence in the following cases:

- At inception of a business relationship with a customer who has not been physically present during the identification procedure (non-face to face customers);
- At inception of a business relationship with a politically exposed person;
- When starting cross-border credit institution relationship with respondents from third countries.

Credit institutions and financial institutions, that are supervised by the FCMC in accordance with the Law, shall also perform enhanced customer due diligence in all cases where any of the high AML risks features have been identified according to data on country of customers registration (residence), type of commercial activity, legal or ownership form, type of financial services received or transactions.

A country or a territory shall be considered as having a high customer residence (registration) country risk where:

- It has been included in the list of low tax or tax free countries and territories as approved by the Cabinet of Ministers;
- The United Nations Organisation or the European Union has established financial or civil legal restrictions in respect of it;
- It has been included in the list of non-cooperating countries of the Financial Action Task Force or that body has published a statement to the effect that the respective country or territory does not have regulatory provisions for combating money laundering or terrorist financing or such provisions fail to comply with international requirements due to material deficiencies. The Financial and Capital Market Commission shall notify financial institutions of such countries and territories.

The following customers who are characterized by high risk of legalization of proceeds from crime or terror financing:

- Legal persons that issue or are entitled to issue bearer shares (equities);
- Legal persons whose ownership or membership structure hampers the detection of the beneficial owner;
- Societies, foundations and legal arrangements equivalent to foundations that are not established for profit-gaining purposes except in the cases when they have been granted the status of public good in the Republic of Latvia;
- External accountants, legal advisors or legal arrangement and company service providers that open accounts on their behalf with financial institutions to perform financial operations on customers' behalf;

- Customers whose commercial or private activities are not related to the Republic of Latvia except in the cases when a customer enters into a business relationship with a branch or a representative office or a parent or a subsidiary undertaking in a foreign country of a financial institution registered in the Republic of Latvia and the customer's commercial or private activities are related to the country where that branch or representative office or the parent or the subsidiary undertaking is located. The said condition shall not refer to the cases when a customer obtains units of an investment fund registered in the Republic of Latvia.

Types of customer's commercial activity characterised by high risk of legalization of criminal proceeds or terror financing risk shall be considered in case of the following types of commercial activity:

- Arrangement of gambling;
- Provision of cash collection services;
- Intermediation in transactions with real estate;
- Trading in precious metals and precious stones;
- Trading in arms and ammunition;
- Provision of reinsurance services except in the cases when the service provider has an appropriate licence and its activity is supervised or it has been granted an assessment in investment category by international rating agencies;
- Provision of money services (e. g., teller desks for payments, foreign exchange offices, money transmission agents or other service providers offering money transmission possibilities).

Products of financial institutions that are characterised by a high risk of legalization of criminal proceeds or terror financing, are:

- Private banking services whereby tailor-made services are provided to wealthy customers, natural persons, by ensuring overall asset management, including advice on financial planning, investment, tax and heritage issues, special lending terms, special procedure whereby these customers and their transactions are serviced and higher confidentiality of customer data;
- Loans secured with a collateral of financial instruments or a guarantee issued by a credit institution of a third country, excluding repo transactions;
- Trust services where the amount transferred for trust exceeds an equivalent of 286 000 EUR;
- Issuing and servicing payment cards provided that a single customer, natural person, orders more than 10 payment cards or a single customer, legal person, orders at least 20 payment cards or a less quantity where the number of payment cards is not related to the economic activity of the customer.

- Transactions effected by customers that are characterised by a high risk of legalization of proceeds from crime or terror financing shall be considered transactions complying with the following description:
  - The payment made or received notably exceeds the threshold set by a financial institution as a result of the due diligence of the customer's economic/personal activity;
  - The monthly credit turnover exceeds an equivalent of 286 000 EUR or notably exceeds another lower threshold set by a financial institution as a result of the due diligence of the customer's economic/personal activity;
  - The three-months credit turnover exceeds an equivalent of 714 000 EUR or notably exceeds another lower threshold set by a financial institution as a result of the due diligence of the customer's economic/personal activity;
  - The yearly credit turnover exceeds an equivalent of 2 857 000 EUR or notably exceeds another lower threshold set by a financial institution as a result of the due diligence of the customer's economic/personal activity;
  - The first credit transaction on the customer's account is made six months after the date of establishing business relationship with the customer and the monthly credit turnover has reached an equivalent of 71 000 EUR;
  - The first outgoing payment from the customer's account is made 12 months after the opening of the account;
  - A cash transaction of a customer, natural person, exceeds an equivalent of 14 000 EUR or the aggregate cash transactions in a month exceed an equivalent of 71 000 EUR, or a cash transaction of a customer, legal person, exceeds the threshold that has been set by a financial institution for such aggregate of cash transactions as a result of the due diligence of the customer's economic activity;
  - A customer is a society or a foundation and within business relationship money is transmitted to a foreign country and the transaction volume exceeds an equivalent of 10 000 EUR.

## [EXISTING GUIDELINES TO THE BANKING INDUSTRY]

By developing appropriate policies and procedures, any legal person subject to the Law shall establish and document an internal control system for the prevention of money laundering and terrorist financing that is commensurate with its operations. An internal control system is a set of measures that includes actions for ensuring compliance with legal requirements by allocating adequate resources and training of the staff with the aim of averting, to the possible extent, the involvement of a person subject to the AML/CTF Law.

When establishing an internal control system, credit institutions, insurance companies and investment brokerage firms shall follow the requirements for the establishment of the internal

control system as set out in the Credit Institution Law, the Law on the Financial Instruments Market, Law on Insurance Companies and Supervision thereof and the FCMC Regulations No. 63, "Regulations for Creation of an Internal Control System".

## [GENERAL FEEDBACK (NEW MODUS OPERANDI, TRENDS, REAL CASES, etc)]

By introducing higher AML/CTF standards during 2005, the number of foreign customers was reduced by 37%! The reduction has mainly been driven by (or is mainly owing to) the requirements to disclose beneficial owners for legal persons and the fact that in other countries such requirements have not yet been introduced. During 2007, the number of foreign customers has increased, however it is still far below levels of 2005.

There is limited feedback from the FIU regarding practical cases of money laundering or terrorist financing to MLROs. Thus commercial banks rely on their own experience and expertise. General feedback commercial banks receive from the Control Service only during AML/CTF training programs.

## [PURPOSES FOR WHICH THE FEEDBACK INFORMATION MAY BE USED]

The feedback from the FIU could be used in order to find latest development and methods of money laundering and terrorist financing. That would allow appropriate change settings for monitoring systems and detect possible additional money laundering and terrorist financing cases.

## [PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK STAFF IN THE EVENT OF NOTIFICATION) OF THE INSTITUTIONS OR PERSONS COVERED BY THIS DIRECTIVE ]

Where, in due course of the Law, a person subject to AML/CTF Law has reported to the FIU in good faith, whether money laundering, terrorist financing or an attempt thereof, or other criminal offence related thereto is proven or not during the course of pre-trial criminal proceedings, or in the court and irrespective of the provisions of the mutual agreement between a customer and the person subject to the Law, disclosure of information to the FIU shall not constitute disclosure of confidential information and shall not incur legal, including civil, liability.

Where a person subject to the AML/CTF Law has refrained from executing a transaction in good faith in accordance with Article 32 hereof, discontinued business relationship or requested fulfilment of liabilities before maturity, refraining from or delaying a transaction, discontinuing a business relationship or requesting fulfilment of liabilities before maturity shall not incur legal, including civil, liability on the person subject to this Law.

Where the FIU has issued an order for the suspension of a transaction in accordance with the requirements of the Law, this shall not incur legal, including civil, liability on the person subject to the Law irrespective of the outcome of the suspension of the transaction.

## [CONSERVATION OF RECORDS AND DOCUMENTS]

A person subject to the Law shall keep the following for at least five years after the termination of the business relationship:

- Copies of documents evidencing customer identification data;
- Information about customers and their accounts;
- Statements about the beneficial owner;
- Correspondence, including by electronic mail;
- Other documents, including in an electronic form, obtained during customer due diligence.

In separate cases, upon an order of the FIU, they may be extended to more than five years, but it shall not exceed six years.

## [STEPS TAKEN TO INCREASE AWARENESS OF THE PHENOMENON OF MONEY LAUNDERING (E.G.: TRAINING, INFORMATION...)]

Association of Latvian Commercial Banks (ALCB) provides AML/CTF education and training courses. Until 31.12.2008, 488 persons successfully passed exams and the Association issued 71 certificates for Basic AML/CTF program, 282 certificates for Advanced AML/CTF program and 135 certificates for Expert AML/CTF program.

In order to develop knowledge and skills of MLROs, the Consulting and Education Centre of ALCB has concluded an agreement with Association of Certified Anti-Money Laundering Specialists (ACAMS). During 2008, first persons successfully passed ACAMS exams.

There are numerous AML/CTF seminars, trainings and education programmes where compliance, monitoring and other banks specialists participate.

From 1998 to 2008, the Control Service has issued 216 publications and provided 209 education programmes regarding AML/CTF.

### [ANTI-MONEY LAUNDERING / CFT LEGISLATION]

The main legislation concerning AML and CFT is written in the “Law on Professional Due Diligence” (Due Diligence Act, DDA). In addition, there are mainly the Criminal Code (“Strafgesetzbuch” abbr. StGB), and the “Law against Market Abuse in the Trading of Financial Instruments” (Market Abuse Act, MAA).

Customer due diligence (CDD) in Liechtenstein is set out in the Due Diligence Act (DDA), which transposed the revised FATF Recommendations, the EU Third Money Laundering Directive (EC Directive 2005/60/EC) and the EC Directive 2006/70/EC, effective 1 March 2008.

Note: The following remarks refer to an unofficial English translation. The German version of the Act is authoritative.

The DDA defines the scope, requirements, and supervision of CDD, and provides for enforcement and information sharing. The legal requirements are expanded and specified in the Government’s Due Diligence Ordinance (DDO).

With entry into force of the Market Abuse Act on 1 February 2007, a regulatory framework has been set up to combat market abuse activities in the Liechtenstein financial centre. The object of this law is to expand the current offence of insider dealing and to introduce the new offence of market manipulation. Insider dealing, in the case of the economic advantage acquired through the offence exceeding 75,000 Swiss francs, is considered as predicate offence to Money Laundering.

Liechtenstein’s Criminal Code, the Strafgesetzbuch (StGB), is modeled on the Austrian Criminal Code. Money laundering is criminalized through § 165 StGB; the financing of terrorism pursuant to § 278b, 278c, and 278d StGB.

### [PENALTIES IN NATIONAL LAW FOR FAILURE TO RESPECT THE NATIONAL PROVISIONS OF THE EU DIRECTIVE]

In Article 30 f. DDA, several penal provisions are stated in the case of criminal offenses (for example for failure in respect of due diligence duties). The Court of Justice can punish anyone with imprisonment of up to six months or with a fine of up to 360 daily rates (of between 10 to

1,000 Swiss francs). For committing an administrative offence, the Financial Market Authority (FMA)<sup>7</sup> can punish the offender with a fine of up to 100,000 Swiss francs.

The provisions of the DDA are without prejudice to criminal liability arising from other criminal law provisions.

Most of the relevant criminal law provisions in connection with combating Money Laundering, Terrorist Financing and criminal organizations can be found in the Criminal Code (StGB).

## [CENTRAL AUTHORITY FOR REPORTING]

The Financial Intelligence Unit (FIU) is the central agency for the collection and analysis of information needed to detect money laundering, predicate offences of money laundering, organized crime, and terrorist financing. The FIU is a Financial Intelligence Unit according to the principles laid down by the Plenary Assembly of the Egmont Group in November 1996 in Rome and amended in June 2004 in Guernsey. The FIU is a separate agency and is not subordinated to any other body, in particular not to the FMA. The FIU exists upstream of the law enforcement authorities and is not part of them. The FIU is the central state agency to which direct and unfiltered Suspicious Activity Reports (SAR) are filed.

The Law on the Financial Intelligence Unit (FIU Act) creates the formal legal basis for the FIU. The content of the FIU Act specifies the competencies and responsibilities, as well as the rights and duties of the FIU in connection with obtaining and analyzing information for the recognition of money laundering, predicate offences of money laundering, organized crime, and terrorist financing.

The FIU serves as an interface between the persons subject to due diligence and the law enforcement authorities (in the first place the Public Prosecutor). Its main task is to analyze the disclosed information in order to establish if there are indications of money laundering, related predicate offences, organized crime, or terrorist financing. There is also a duty of the persons who are dealing professionally with financial instruments and who are therefore subject to due diligence to submit a report to the FIU if they suspect that a transaction might constitute insider dealing or market manipulation.

The government has, as well, established a Counter-Terrorism Coordination Task Force, headed by the FIU, and including the FMA, national police, public prosecutor, legal assistance unit, judicial service, personal staff to the government (directly reporting to the prime minister), foreign ministry, and the Government's Press Office.

---

<sup>7</sup> The FMA is an integrated financial supervisory authority for all financial markets and institutions and providers of financial services. Its objectives are to safeguard the stability of the Liechtenstein financial center, the protection of clients, the prevention of abuses, and compliance with international standards.

## [PERSONS RESPONSIBLE FOR REPORTING]

The persons subject to due diligence must appoint a contact person for the responsible authority as well as persons or expert bodies for the internal functions of compliance officers and investigating officers (Article 22 DDA).

In accordance with Article 17 DDA, a suspicious activity report (SAR) in writing must be immediately submitted to the FIU by the persons subject to due diligence should the suspicion exist that a connection is given to money laundering, a predicate offence of money laundering, organized crime, or the financing of terrorism, either as such or as a result of special inquiries that validate the suspicions of money laundering, related in some circumstances or transactions (Article 9 paragraph 4 DDA).

All suspicious transactions or activities must be reported to the FIU pursuant to Article 17 DDA, regardless of the financial amount involved. There is no minimum reporting threshold.

## [BUSINESS COVERED BY THE LEGISLATION (WHICH SPECIFIC PERSONS: NOTARIES, LAWYERS...)]

Pursuant to Article 3, the DDA applies to the following legal and natural persons (persons subject to due diligence):

- a) banks and investment firms licensed under the Banking Act;
- b) e-money institutions licensed under the E-Money Act;
- c) management companies licensed under the Investment Undertakings Act;
- d) insurance undertakings licensed under the Insurance Supervision Act, to the extent they offer life insurance;
- e) the Liechtenstein Postal Service (limited company), to the extent it pursues activities beyond its universal service that must be notified to the FMA;
- f) exchange offices;
- g) insurance brokers licensed under the Insurance Mediation Act, to the extent they broker life insurance contracts and other services for investment purposes;
- h) payment service providers;
- i) asset management companies licensed under the Asset Management Act;
- k) professional trustees and trust companies licensed under the Professional Trustees Act, to the extent they pursue activities under Article 7 paragraph 1 (a), (b), (e) or audit

activities under (f) or activities under Article 7 paragraph 2 of the Professional Trustees Act;

l) casinos when granting admission to visitors, regardless of whether the visitor actually takes part in gaming activities or buys or sells gaming tokens;

m) lawyers and law firms entered in the lists of lawyers or lists of law firms under the Lawyers Act as well as legal agents as referred to in Article 67 of the Lawyers Act, to the extent they provide tax advice to their clients or assist in the planning or execution of transactions for their client concerning the:

- buying and selling of undertakings or real property;
- managing of client money, securities or other assets;
- opening or management of accounts, custody accounts or safe deposit boxes;
- organization of contributions necessary for the creation, operation or management of legal entities; or
- establishment of a legal entity on the account of a third party or acting as a partner of a partnership or a governing body or general manager of a legal entity on the account of a third party or carrying out a comparable function on the account of a third party;

n) natural and legal persons licensed under the Law on Auditors and Auditing Companies as well as audit offices subject to specialized legislation;

o) holders of a certification under Article 180a of the Law on Persons and Companies (PGR), to the extent that they act as a partner of a partnership or a governing body or general manager of a legal entity on the account of a third party or carry out a comparable function on the account of a third party;

p) real estate agents, to the extent that their activities cover the purchase or sale of real property;

q) natural and legal persons trading in goods on a professional basis, to the extent that payment is made in cash in an amount of 25,000 Swiss francs or more, whether the transaction is executed in a single operation or in several operations which appear connected;

r) natural and legal persons, to the extent that they provide a registered office, business address, correspondence or administrative address and other related services for a legal entity on a professional basis;

s) natural and legal persons, to the extent that they act as a nominee shareholder for another person other than a company listed on a regulated market that is subject to disclosure requirements in conformity with EEA law or subject to equivalent international standards, or to the extent that they provide the possibility for another person to carry out that function. The FMA shall issue a list of countries with equivalent regulations;

t) natural and legal persons who, on a professional basis and on the account of a third party, act as a partner of a partnership or a governing body or general manager of a legal entity or carry out a comparable function on the account of a third party;

u) natural and legal persons who, on a professional basis, accept or keep third-party assets or assist in the acceptance, investment, or transfer of such assets or who, on a professional basis, carry out external accounting and audits.

Liechtenstein branches of foreign undertakings referred to in paragraph 1 are also deemed persons subject to due diligence, to the extent such branches are permissible.

## [PREDICATE OFFENCES COVERED]

Liechtenstein has adopted a combined approach, listing all felonies and a number of misdemeanours in § 165 StGB as predicate offences of money laundering. Felonies are intentional offences sanctioned with life imprisonment or imprisonment of more than three years (§ 17 StGB), whereby the maximum sanction is the determining factor for the differentiation between felonies or misdemeanours. Misdemeanours listed as predicate offences for money laundering relate to terrorist financing, corruption and bribery, smuggling, forgery, misconduct by public officials, offences in terms of Article 76 of the Law concerning Value Added Tax, offences in terms of Articles 83 - 85 of the Foreigners Act, and offences of the Narcotics Act, including sale or procurement of narcotics, financing narcotics trafficking, or the procurement of financing of narcotics.

## [IDENTIFICATION]

### a. *Definition (e.g.: PEPs, beneficial owner, thresholds...)*

**Beneficial owners** are defined in Article 2 paragraph 1 (e) DDA:

A natural person on whose initiative or in whose interest a transaction or activity is carried out or a business relationship is ultimately constituted. In the case of legal entities, the beneficial owner is also the natural person in whose possession or under whose control the legal entity ultimately is situated.

**Politically-exposed persons (PEPs)** are defined in Article 2 paragraph 1 (h) DDA:

Natural persons who are or have, until a year ago, been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons.

**b. Identification threshold amount**

**Contracting parties** and beneficial owners must be identified when entering into a business relationship (Article 5 f. DDA). Identification requirements apply to contracting parties, without any restriction based on their legal status. No distinction is made between occasional and permanent relationships, but minimum thresholds are set for occasional transactions.

The persons subject to due diligence must identify the beneficial owner. By means of risk-based and adequate measures, they must verify the identity of the beneficial owner to satisfy themselves that this is actually the beneficial owner. In the case of a legal entity, this includes risk-based and adequate measures to determine the ownership and control structure of the contracting party.

If, over the course of the business relationship, doubts arise concerning the identity of the beneficial owner, the persons subject to due diligence must repeat the identification and verification of the identity of the beneficial owner.

**c. Identification at a distance (non face to face)**

Article 11 DDA:

Business relationships where the contracting party was not personally present for identification are considered cases with higher risk, so that the identity of the contracting party must be proven by means of additional measures.

**d. Outsourcing of identification to third parties**

Pursuant to Article 14 DDA, persons subject to due diligence may entrust another person subject to due diligence or a natural or legal person abroad that is subject to Directive 2005/60/EC or equivalent regulation and supervision to carry out the identification of the contracting party and of the beneficial owner and the compilation of the profile.

In case of joint services (Article 15 DDA), the person subject to due diligence responsible for the mandate can perform all CDD for all persons subject to due diligence concerned. Even in cases where due diligence is performed by a third party, the responsibility for compliance with CDD provisions remains with the persons subject to due diligence. Access to due diligence files must be granted at any time to the other persons subject to due diligence (Article 15 paragraph 3 DDA).

**e. Means of identification**

Article 6 paragraph 1 DDA stipulates that the persons subject to due diligence must identify the contracting party and verify the contracting party's identity by means of confirmatory documents.

For natural persons, confirmatory documents are valid official identity papers with a photograph (especially passport, identity card, or driver license). Identity papers are considered valid if, at the time the contracting party is identified and the identity is verified, they would entitle the contracting party to enter the Principality of Liechtenstein. If the contracting party is unable to obtain such a document, the contracting party must present certification of identity from the competent authority of his place of residence.

For legal entities entered in the Public Registry, confirmatory documents are an extract from the Public Registry issued by the Office of Public Registration; a written extract from a database administered by the Office of Public Registration; or a written extract from a trustworthy, privately administered directory or equivalent database.

For legal entities not entered in the Public Registry, confirmatory documents are a domestic official certification; the articles of association, formation deeds, or the formation contract; certification of the information by the elected statutory auditor; an official license to engage in business activities; or a written extract from a trustworthy, privately administered directory or equivalent database.

**f. Form and treatment of the documents**

If a business relationship is taken up by way of correspondence, the persons subject to due diligence must include the original or the certified copy of the confirmatory document in the due diligence files. If, in order to identify the contracting party and verify the contracting party's identity, the person subject to due diligence has the original of a confirmatory document presented by a person who can issue a certification of authenticity, the person subject to due diligence may also proceed as follows: Upon taking up a business relationship or carrying out an occasional transaction by way of personal appearance, it shall suffice if the persons subject to due diligence make a copy of the original or of the certified copy, confirm on that copy that the original or the certified copy has been examined, sign and date the copy, and include it in the due diligence files.

The documents required to verify identity must reflect current circumstances. Certifications of authenticity, registry extracts, and certifications by the elected statutory auditor may not be older than 12 months.

**g. Source of information (e.g.: public register for the identification of beneficial owner)**

See above.

## [PRODUCTS AND TRANSACTIONS CHARACTERISED BY A HIGH/LOW RISK OF MONEY LAUNDERING]

In their internal instructions, the persons subject to due diligence must establish criteria designating business relationships and transactions with higher risk and allocate the respective business relationships and transactions accordingly.

In the following cases, business relationships and transactions must always be assumed to have higher risks:

- In business relationships where the contracting party was not personally present for identification, the identity of the contracting party must be proven by means of additional measures.
- With regard to business relationships and transactions with politically exposed persons, the persons subject to due diligence must:
  - employ adequate, risk-based procedures to determine whether the contracting party or the beneficial owner is a politically exposed person or not;
  - obtain the approval of at least one member of the general management before establishing a business relationship with such a contracting party or beneficial owner or – where a contracting party or a beneficial owner is recognized as a politically exposed person in the context of an existing business relationship – before continuing the business relationship;
  - each year, obtain the approval of at least one member of the general management in order to continue business relationships with politically exposed persons.
- In respect of cross-border correspondent banking relationships with respondent institutions from a third State, persons subject to due diligence under article 3 paragraph 1 (a) to (h) must ensure that they:
  - have sufficient information about the respondent institution to understand the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision;
  - assess the respondent institution's anti-money laundering and anti-terrorist financing controls;
  - obtain approval from at least one member of the general management before establishing new correspondent banking relationships;

- document the respective responsibilities with respect to fulfillment of due diligence requirements by the two institutions involved.

In addition, following a consultation with the FIU, the FMA has issued a guideline concerning indicators for money laundering.

## [EXISTING GUIDELINES TO THE BANKING INDUSTRY]

The Banking Act (BA) and the Banking Ordinance (BO) define and regulate banking activities and entrust the FMA with supervisory powers. BA and BO do not specifically address AML/CFT issues, but request banks to set up internal guidelines governing powers and procedures for risk management issues, including operational and legal risks (Article 7.a BA), and to conduct sound and proper business operations (Article 19 BA).

In the field of AML/CFT, the FMA has issued two guidelines, one concerning monitoring of business relationships and one dealing with due diligence inspections conducted by mandated due diligence auditors.

## [[GENERAL FEEDBACK (NEW MODUS OPERANDI, TRENDS, REAL CASES, ETC)]]

After each Suspicious Activity Report (SAR), the FIU gives a case by case feedback to the reporting entity.

The FIU offers training through participation of its staff in training sessions organised by different organisations, such as the Institute for Compliance and Quality Management (ICQM) and the University of Liechtenstein.

In each annual report of the FIU, a case study is presented and general feedback on trends and typologies is given.

## [PURPOSES FOR WHICH THE FEEDBACK INFORMATION MAY BE USED]

On the one hand, the feedback is used to improve continuously the system, while on the other hand, it serves as an early detection and awareness-raising instrument.

## [PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK STAFF IN THE EVENT OF NOTIFICATION) OF THE INSTITUTIONS OR PERSONS COVERED BY THIS DIRECTIVE ]

Article 19 paragraph 1 DDA: If a person has submitted a report to the FIU and the report turns out to have been unjustified, such a person shall be free of any liability under civil or criminal law, unless the person was acting intentionally. In the same way, there shall be no civil liability for persons not discontinuing a business relationship in accordance with paragraph 2, even though the contracting party expressly wishes a discontinuation or termination of the business relationship.

## [CONSERVATION OF RECORDS AND DOCUMENTS]

The persons subject to due diligence must document their compliance with the due diligence requirements and the reporting obligation in accordance with the DDA. For that purpose, they must keep and maintain due diligence files. Client-related records and receipts shall be kept for at least ten years from the end of the business relationship or conclusion of the occasional transaction; transaction-related records and receipts, on the other hand, for at least ten years from the conclusion of the transaction or from their preparation. In cases of simplified due diligence, the person subject to due diligence must document the reason for exemption from due diligence in the due diligence files.

The due diligence files must in particular contain the records and receipts compiled and consulted for purposes of complying with the provisions of the DDA and the DDO. They must in particular include: the documents and records that served to identify and verify the identity of the contracting party and the beneficial owner; the business profile; the documentation on any clarifications and all documents, records, and receipts consulted in this connection; records indicating transactions and, if applicable, assets; and any reports submitted to the FIU.

The due diligence files must be compiled and kept in a way that the required due diligence can be performed at any time; that they enable specialized third parties to reach a reliable judgement on compliance with the provisions of the DDA and the DDO; and that requests by competent domestic authorities and courts, auditors and audit offices can be fully complied with within a reasonable period of time.

Due diligence files may only be kept in Liechtenstein.

During criminal procedures, the prosecuting authorities are empowered to confiscate or to seal the documents, according to Article 96 of the StPO (Strafprozessordnung = Code of criminal procedure), and extend the retention period.

[STEPS TAKEN TO INCREASE AWARENESS OF THE PHENOMENON OF MONEY LAUNDERING (E.G.: TRAINING, INFORMATION...)]

Ongoing employee training on AML/CFT matters: Persons subject to due diligence must ensure initial and ongoing training of their staff according to the DDA. This training covers requirements to prevent and combat money laundering, predicate offences of money laundering, organized crime, and the financing of terrorism.

The FMA supervises compliance with the legal training obligations.

The FIU and the FMA practices training activities, both through participation of its staff in various training courses, especially those of the Institute for Compliance and Quality Management (ICQM) and of the Business Sciences department of the University of Liechtenstein, along with other events. The goal of these efforts is to expand further sensitization of the persons subject to due diligence.

ICQM is an initiative of the associations representing the financial sector in Liechtenstein (among others: Bankers' Association, Association of the fiduciaries, Association of the wealth managers, Fund manager Association, and Association of accountants). The training seminars are conducted in cooperation with TvT compliance Ltd, an internationally operating compliance solution provider, with offices in Liechtenstein and Switzerland.

### [ANTI-MONEY LAUNDERING /CTF LEGISLATION]

- The law of 9 July 1989, which amends the amending law of 19 February 1973 on the Sale of Medication and the Prevention of Drug Addiction. This law introduces the principle of drug-related money laundering as a criminal offence.
- The law of 5 April 1993 on the financial sector. This law transposes the European Money Laundering Directive into national law. The law sets out the behaviour to be adopted by financial sector professionals as regards money laundering.
- The grand-ducal decree of 6 January 1995 authorising the creation and operating of a database containing information and notifications from credit institutions and other financial sector professionals, as well as from life insurance companies and insurance brokers on facts and transactions likely to be related to money laundering resulting from drug trafficking.
- The law of 11 August 1998 introducing the incrimination of criminal organisations and the offence of money laundering into the Penal Code and amending:
  - the amended law of 19 February 1973 concerning the sale of medicinal substances and the fight against drug addiction;
  - the amended law of 5 April 1993 relative to the financial sector;
  - the amended law of 6 December 1991 relative to the insurance sector;
  - the amended law of 9 December 1976 relative to the organisation of notaries public;
  - the law of 20 April 1977 relative to games of chance and betting on sports events;
  - the law of 28 June 1984 regulating the profession of company auditors;
  - the rules of criminal procedure.
  - This law introduces the prohibition of money laundering into a new section of the Penal Code. It has a twofold objective:
    - to extend the scope of application of the offence of money laundering to offences other than those related to drug trafficking (criminal organisations, arm trafficking etc.);
    - to extend the system concerning the prevention and detection of money laundering, hitherto limited to the financial sector, to other sectors likely to be involved in money laundering operations or confronted with such operations.

- The law of 31 May 1999 governing the domiciliation of companies and:
  - amending and completing certain provisions of the amended law of 10 August 1915 concerning trading companies;
  - amending and completing certain provisions of the amended law of 23 December 1909 concerning the creation of a trade and company register;
  - amending and completing the amended law of 28 December 1988 regulating access to professions in the craft industries, the professions of merchant and industrialist as well as to other professions;
  - completing the law of 12 July 1977 relative to holding companies;
  - amending and completing certain provisions of the law of 5 April 1993 relative to the financial sector;
  - completing the amended law of 6 December 1991 on the insurance sector.
  
- The law of 10 June 1999 governing the organisation of the profession of chartered accountant.
  
- The law of 15 January 2001 transposing the OECD Convention of 21 November 1997 on combating bribery of foreign public officials in international business transactions.
  
- The law of 14 June 2001 transposing the Convention on laundering, search, seizure and confiscation of the proceeds from crime, signed in Strasbourg on 8 November 1990.
  
- The law of 1 August 2001 concerning the € changeover on 1 January 2002 and amending certain provisions laid down by law.
  
- The law of 12 November 2004 concerning the fight against money laundering and terrorist financing and embodying Directive 2001/97/CE amending Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering.
  
- The Law of 17 July 2008 on the fight against money laundering and terrorist financing and amending article 506-1 of the Penal Code and the Law of 14 June 2001:  
The list of predicate offences of money laundering is extended to all offences punishable by a detention order for a minimum of more than six months.
  
- The Law of 17 July 2008 transposing Directives 2005/60/EC and 2006/70/EC and amending:

- The Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended;
- The Law of 7 March 1980 on the organisation of the judicial system, as amended;
- The Law of 5 April 1993 on the financial sector, as amended;
- The Law of 6 December 1991 on the insurance sector, as amended;
- The Law of 9 December 1976 on the profession of notary, as amended;
- The Law of 10 August 1991 on the profession of lawyer, as amended;
- The Law of 28 June 1984 on the organisation of the profession of company auditor, as amended;
- The Law of 10 June 1999 on the organisation of the profession of accountant.

## [PENALTIES IN NATIONAL LAW FOR FAILURE TO RESPECT OF THE NATIONAL PROVISIONS TO THE DIRECTIVE]

Article 9 of the Law of 17 July 2008 provides a fine from 1250 to 125000 euros for non-compliance with the law.

## [CENTRAL AUTHORITY FOR REPORTING]

The Public Prosecutor for the Luxembourg Court must be informed of any fact that could be an indication of money laundering. A copy of each suspicious transaction report has to be sent to the supervisory authority for banks (CSSF).

## [PERSONS RESPONSIBLE FOR REPORTING]

Article 5 of the Law of 17 July 2008 requires the professionals to appoint one or several persons responsible for forwarding data to the authorities. Data are in practice communicated by one or more persons designated for this purpose by the professionals subject to money laundering legislation.

## [BUSINESS COVERED BY THE LEGISLATION (WHICH SPECIFIC PERSONS: NOTARIES, LAWYERS...)]

The obligation to inform the authorities of any suspicion of possible money laundering transactions now extends to the following professionals:

- investment firms;

- financial operations advisers;
- brokers;
- market makers;
- professional custodians of securities or other financial instruments;
- corporate domiciliation agents;
- operators of payment systems or clearing systems for securities transactions;
- currency exchange offices;
- debt recovery organisations;
- client communication agents;
- administrative agents of the financial sector;
- operators of EDP systems and communication networks of the financial sector;
- professionals providing company incorporation and management services;
- insurance companies;
- notaries;
- casinos and gaming establishments;
- company auditors;
- accountants;
- pension funds under the prudential supervision of the “*Commissariat aux Assurances*”;
- persons agreed to undertake the management of pension funds under the prudential supervision of the “*Commissariat aux Assurances*”;
- insurance intermediaries agreed in Luxembourg or authorised to exercise their activities in Luxembourg;
- undertakings for collective investment marketing their units, or shares and defined under the law of 20 December 2002 relating to undertakings for collective investment, or under the law of 30 March 1988 relating to undertakings for collective investment, or under the law of 19 July 1991 relating to undertakings for collective investment, the securities of which, are not intended to be placed with the public;
- management companies subject to the law of 20 December 2002 relating to undertakings for collective investment and marketing units or shares of undertakings for collective investment or carrying out additional or auxiliary activities within the meaning of the law of 20 December 2002 relating to undertakings for collective investment;
- pension funds under the prudential supervision of the “*Commission de Surveillance du*”

Secteur Financier” (supervisory authority of the financial sector);

- professionals as referred to in article 13 of the law of 5 April 1993 on the financial sector:
  - persons providing an investment service where that service is provided in a secondary manner in the course of a professional activity regulated by legal or regulatory provisions or a code of ethics;
  - undertakings, which provide investment services exclusively for their parent undertakings and subsidiaries;
  - undertakings, which provide a service under chapter 2 of the law of 5 April 1993 on the financial sector, other than an investment service;
  - undertakings, which provide investment services consisting exclusively in the administration of employee-participation schemes;
  - advisers and managers of Luxembourg collective investment undertakings;
  - persons whose main business consists of dealing in raw materials between themselves or with persons or entities producing or using those products for business purposes, and who provide investment services only to those counterparties, and to the extent necessary, for the carrying on of their main business;
  - undertakings which provide investment services consisting exclusively in dealing for their own account on financial-futures or options markets, or which deal for the accounts of other members of those markets or make prices for them;
  - real estate agents established or acting in Luxembourg;
  - lawyers within the meaning of the amended law of 10 August 1991 on the profession of lawyer when they:
    - a) assist in the planning or execution of transactions for their client concerning the;
    - b) buying or selling of real property or business entities;
    - c) managing of client money, securities, or other assets;
    - d) opening or management of bank, savings, or securities accounts;
    - e) organisation of contributions necessary for the creation, operation, or management of companies;
    - f) creation, operation, or management of trusts, companies and similar structures;
    - g) or by acting on behalf of and for their client in any financial or real estate transaction;
- persons, others than those mentioned here above, carrying out in Luxembourg on a professional basis the activity of fiscal consultancy, economic consultancy or one of the activities described under a) and b) of the previous item;

- natural or legal persons trading in goods, whenever payment is made in cash, and in an amount of €15, 000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked.
- trust or company service providers.

## [PREDICATE OFFENCES COVERED]

The predicate offences are as follows:

- drug trafficking;
- abduction of minors;
- sexual offences against minors;
- procuring;
- fraud on the financial interests of the State and of international institutions;
- corruption (private and public sector);
- violation of the legislation on arms and munitions;
- crimes and offences committed in the context of, or in relation to, an association formed with a view to attempting the commission of offences against persons or property or in the context of, or in relation to, a criminal organisation;
- acts of terrorism and terrorist financing;
- the counterfeiting and falsification of seals, stamps, punches, marks, coins and banknotes;
- the use and disclosure of trade secrets or manufacturing secrets;
- theft;
- bankruptcy;
- embezzlement;
- fraud;
- illicit trafficking in stolen goods and other goods;
- illicit trafficking in migrants,
- infringement of copyright,
- crimes and offences against the environment;
- smuggling;

- the offences of insider trading and market manipulation;
- any other offence punishable by a minimum term of imprisonment longer than six months.

## [IDENTIFICATION]

### a. **Definition (e.g.: PEPs, beneficial owner, thresholds...)**

The Law of 17 July 2008 resumes definitions of the Directive 2005/60/EC, in particular:

- **“beneficial owner”** means the natural person(s) who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted. The beneficial owner shall at least include:
  - a) In the case of corporate entities:
    - the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards; a percentage of 25% plus one share be deemed sufficient to meet this criterion;
    - the natural person(s) who otherwise exercises control over the management of a legal entity;
  - b) in the case of legal entities, such as foundations, and legal arrangements, such as trusts, which administer and distribute funds:
    - where the future beneficiaries have already been determined, the natural person(s) who is the beneficiary of 25% or more of the property of a legal arrangement or entity;
    - where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;
    - the natural person(s) who exercises control over 25% or more of the property of a legal arrangement or entity.
- **“politically exposed persons”** means natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons;

- **"trust and company service providers"** means any natural or legal person which by way of business provides any of the following services to third parties:
  - forming companies or other legal persons;
  - acting as or arranging for another person to act as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
  - providing a registered office, business address, correspondence or administrative address and other related services for a company, a partnership or any other legal person or arrangement;
  - acting as or arranging for another person to act as a trustee of an express trust or a similar legal arrangement;
  - (e) acting as or arranging for another person to act as a nominee shareholder for another person other than a company listed on a regulated market that is subject to disclosure requirements in conformity with Community legislation or subject to equivalent international standards.
- **"business relationship"** means a business, professional or commercial relationship which is connected with the professional activities of the institutions and persons covered by this Directive and which is expected, at the time when the contact is established, to have an element of duration;
- **"shell bank"** means a credit institution, or an institution engaged in equivalent activities, incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated financial group.

**b. Identification threshold amount**

With regard to occasional customers (where there is no account relationship) identification procedures must be carried out for any operation which amounts to or exceeds € 15,000. Financial sector professionals are obliged to demand identification, even where the amount of the transaction is below the € 15,000 threshold, where there is suspicion of money laundering.

**c. Identification at a distance (non-face to face)**

Professionals have to take specific and adequate measures necessary to compensate for the greater risk of money laundering which arises when establishing business relations or entering into transaction with a customer who has not been physically present for identification purposes (non-face to face operations). Such measures shall ensure that the customer's identity is established, for example, by requiring additional documentary evidence, or supplementary measures to verify or certify the documents supplied, or confirmatory certification by a financial institution, or by requiring that the first payment of the operations is carried out through an

account opened in the customer's name with a credit institution subject to equivalent identification requirements. The internal control procedures shall take specific account of these measures.

**d. Outsourcing of identification to third parties**

Article 3-3 of the law of 17 July 2008 provides that the national or foreign credit institutions and financial institutions company auditors, notaries, other independent legal professionals, and trust or company service providers, subject to equivalent identification requirements are the only acceptable delegates. However, the ultimate responsibility for meeting those requirements shall remain with the institution which relies on the third party.

Third parties shall make information requested immediately available to the institution to which the customer is being referred. Relevant copies of identification and verification data and other relevant documentation on the identity of the customer or the beneficial owner shall immediately be forwarded, on request, by the third party to the institution to which the customer is being referred.

**e. Means of identification**

- Natural persons: Customer identification must be based on official identity documents and must be detailed (surname, first name, address).
- Legal persons: Appropriate officially-approved identification documents (Commercial Register, articles of association, published accounts, etc).
- Natural or legal persons acting for the account of a third person: Where there is doubt, or uncertainty, as to whether a natural person is acting for his own account, financial sector professionals must take reasonable steps to obtain information on the true identity of the persons for whom the customer is acting.

**f. Source of information (e.g.: public register for the identification of beneficial owner)**

The pertinent information or data on the client, the beneficial owners, and on the control of legal persons, may be obtained from public registers, from the customers, or other reliable sources.

[PRODUCTS AND TRANSACTIONS CHARACTERISED BY A HIGH/LOW RISK OF MONEY LAUNDERING]

Article 3-2 of the Law of 17 July 2008 requires the professionals to apply, on a risk-sensitive basis, enhanced customer due diligence measures, in addition to the measures referred to in article 3, in situations which by their nature can present a higher risk of money laundering or terrorist financing.

When the customer has not been physically present for identification purposes, professionals must take specific and adequate measures to composite for the higher risk, for example by applying one more of the following measures:

- a) ensuring that the customer's identity is established by additional documents, data or information;
- b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institutions
- c) ensuring that the first payment of the operations is carried out through an account opened in the customer's name with a credit institution.

In respect of cross-frontier correspondent banking relationships with respondent institutions from third countries, credit institutions must:

- a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision;
- b) assess the respondent institution's anti-money laundering and anti-terrorist financing controls;
- c) obtain approval from senior management before establishing new correspondent banking relationships;
- d) establish by document the respective responsibilities of each institution;
- e) with respect to payable-through accounts, be satisfied that the respondent credit institution has verified the identity of, and performed ongoing due diligence on the customers having direct access to accounts of the correspondent, and that it is able, upon request, to provide relevant customer due diligence data to the correspondent institution,.

In respect of transactions or business relationships with politically exposed persons residing in another Member State or in a third country, credit institutions must:

- a) have appropriate risk-based procedures to determine whether the customer is a politically exposed person;
- b) have senior management approval for establishing business relationships with such customers;
- c) take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction;
- d) conduct enhanced ongoing monitoring of the business relationship.

Credit institutions are prohibited from entering into or continuing a correspondent banking relationship with a shell bank or with a known bank to permit its account to be used by a shell bank.

Professionals are held to pay special attention to any money laundering or terrorist financing threat that may arise from products or transactions that might favour anonymity, and to take measures if needed, to prevent their use for money laundering or terrorist financing purposes.

## [EXISTING GUIDELINES TO THE BANKING INDUSTRY]

The ABL has edited a “*Vademecum of the professional obligations relating to money laundering and terrorist financing*”: this document is intended to assist credit institutions and other financial sector professionals in the effective performance of their obligations, in accordance with the statutory and regulatory provisions applicable in the matter, and to provide various details regarding the practical implementation of the legislation.

## [PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK STAFF IN THE EVENT OF NOTIFICATION) OF THE INSTITUTIONS OR PERSONS COVERED BY THIS DIRECTIVE ]

Under article 5(1) of the Law of 17 July 2008, professionals are held to cooperate with Luxembourg authorities responsible for the combat against money laundering and financing terrorist.

Identity of employees providing the information is held confidential by the authorities, unless its disclosure is necessary to ensure the regularity of the legal proceedings or to ensure the evidence of the facts forming the base of these proceedings.

## [CONSERVATION OF RECORDS AND DOCUMENTS]

Under article 3(6) of the Law of 17 July 2008, professionals are held to keep the following documents, or information, for use in any investigation into, or analysis of, possible money laundering or terrorist financing by Luxembourg authorities responsible for the combat against the money laundering and terrorist financing:

- a) in the case of the customer due diligence, a copy or the references of the evidence required, for a period of at least five years after the business relationship with their customer has ended, without prejudice to longer periods of conservation prescribed by the other laws;
- b) in the case of business relationships and transactions, the supporting evidence and records, consisting of the original documents or copies admissible in court proceedings under the applicable Luxembourg legislation for a period of at least five years

following the carrying-out of the transactions or the end of the business relationship, without prejudice to longer periods of conservation prescribed by the other laws.

[STEPS TAKEN TO INCREASE AWARENESS OF THE PHENOMENON OF MONEY LAUNDERING (E.G.: TRAINING, INFORMATION...)]

Training in the fight against money laundering has always been an integral and important part of the ongoing training provided for bank staff, and this includes in particular that offered by the *Institut de Formation Bancaire, Luxembourg* (IFBL). The Institute's mission is to promote professional skills in the banking and financial fields. Ongoing training is an essential element in the development of Luxembourg as a financial market-place, not least because its reputation as such must necessarily be based on know-how and professionalism on the part of those who work in that market-place.

### [ANTI-MONEY LAUNDERING /CTF LEGISLATION]

- The Prevention of Money Laundering Act of 1994 (as amended).
- The Prevention of Money Laundering and Funding of Terrorism (Regulations) of 2008.<sup>8</sup>
- The Dangerous Drugs Ordinance, Cap.101 (as amended).
- Gaming Act Regulations of 1998 (as amended).

### [PENALTIES IN NATIONAL LAW FOR FAILURE TO RESPECT THE NATIONAL PROVISIONS TO THE DIRECTIVE]

Regulation 4 establishes the obligations to have systems in place and to provide the necessary training to prevent money laundering and the funding of terrorism. In brief, Regulation 4 requires subject persons (i) to have procedures in place for customer due diligence, record keeping, and reporting of suspicious transactions; (ii) to have measures to apply these procedures consistently including in non-face to face transactions; (iii) to establish effective and adequate procedures on internal control, risk assessment and management, compliance and communications; (iv) to provide training to employees including awareness on the domestic legislation and regulations; and (v) to ensure effective screening procedures when hiring employees. Sub-regulation 5 of the regulation establishes penalties for non-compliance with the foregoing. A person found guilty of non-compliance shall, on conviction, be liable to a fine not exceeding €50,000 or to imprisonment for a term not exceeding two years or to both fine and imprisonment.

Regulation 5 provides that when such an offence is committed by a body or other association of persons, corporate, or unincorporated, every person who at the time of the commission of the offence was a director, manager, secretary or other similar officer of such body or association, or was purporting to act in any such capacity, shall *prima facie* be guilty of that offence, unless he proves otherwise. Moreover, Regulation 5 provides that such a body or association of persons shall be liable to an administrative penalty of not less than €1,200 and not more than €5,000. Such an administrative penalty can be imposed by the Financial Intelligence Analysis

---

<sup>8</sup> The 2008 Regulations were published and came into force on 31<sup>st</sup> July 2008. The regulations transpose in totality the EU Third Directive (2005/60/EC) and the Implementing Directive (2006/70/EC)

Unit either as a one time penalty or on a cumulative basis provided the accumulated penalty does not exceed €50,000.

## [CENTRAL AUTHORITY FOR REPORTING]

According to sub-regulation 6 of Regulation 15, knowledge or suspicion of money laundering should be reported to the Financial Intelligence Analysis Unit (FIAU).

The FIAU is a Government agency within the Ministry of Finance, the Economy and Investment, having a distinct legal personality. It is an administrative type of financial intelligence unit and is structured on the Egmont Group FIU model, of which the Unit has been a member since 2003. The FIAU is the national central authority responsible for the collection, processing, analysis, and dissemination of financial information with a view to combating money laundering and the financing of terrorism.

## [PERSONS RESPONSIBLE FOR REPORTING]

The Regulations define a *subject person* as any legal or natural person carrying out either relevant financial business or a relevant activity as defined below (See “Business Covered by the Legislation”). All subject persons are required, under the Regulations, to report suspicious transactions or activities. In this regard, all subject persons must appoint a Reporting Officer to receive internal reports of suspicious operations. The Reporting Officer must consider, in the light of all available information, any reports made to him, and will have reasonable access to any information held by the bank which may assist him for the purpose of considering the report. Where so determined by the Reporting Officer, the report will be submitted to the FIAU within five working days from when the suspicion first arose. The regulations further require that where the Reporting Officer, for justifiable reasons, determines not to report to the FIAU, the Reporting Officer shall record the reasons for such determination in writing, and upon request, make such information available to the FIAU or a supervisory authority acting on behalf of the FIAU.

## [BUSINESS COVERED BY THE LEGISLATION (WHICH SPECIFIC PERSONS: NOTARIES, LAWYERS...)]

The Act covers all persons.

The Regulations cover all persons and institutions undertaking “*relevant financial business*” or a “*relevant activity*”.

“*Relevant financial business*” includes: banking, insurance or investment-related business, as well as foreign exchange bureaux and stockbrokers.

“*Relevant activity*” includes non-financial businesses and professions such as auditors, external accountants and tax advisors, real estate agents, notaries and other independent legal

professionals when assisting their clients in the planning, management, or execution of certain financial investment and real estate transactions, trust and company service providers, casino licensees, and traders when payment is made in cash in an amount equal to € 15,000.

## [PREDICATE OFFENCES COVERED]

Crimes specified in Article 3(1)(a) of the 1988 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, as well as any criminal offence under the laws of Malta.

## [IDENTIFICATION]

### **a. Definition (e.g.: PEPs, beneficial owner, thresholds...)**

Identification is one element of the Customer Due Diligence process. The Regulations require identification, and verification of the identity of all applicants for business and beneficial owners (as defined); directors or other persons vested with the administration and representation of legal entities or arrangements must also be identified.

Identification must be obtained:

- at the start of all business relationships;
- in any transaction exceeding the threshold amount of €15,000 or an occasional transaction involving a money transfer or remittance exceeding €1,000;
- in the case of a series of transactions that in aggregate would exceed the threshold of €15,000;
- where money laundering is suspected, regardless of the amount involved.

Customer acceptance policies and procedures must also be in place to enable subject persons to determine whether the applicant for business is a politically exposed person.

### **b. Identification threshold amount**

Further to the mandatory application of the identification and verification process at the start of all business relationships, the identification threshold amount of EUR 15,000 applies to one-off transactions or to a series of transactions that appear to be connected.

**c. Identification at a distance (non face to face)**

Regulation 11 provides the obligation of the application of enhanced due diligence in circumstances as defined by the regulations. Institutions offering any type of financial service at a distance are therefore required to implement additional procedures to identify positively the customer, including the beneficial owner, and to confirm and verify details. Thus, Regulation 11 requires that, in addition to the standard customer due diligence process as established under Regulation 7, in the case of non-face-to-face identification, subject persons are to apply one or more additional measures as follows, in order to compensate for the higher risk: (i) use additional documentation and information for identification purposes; (ii) verify or certify the documentation supplied through supplementary measures; (iii) obtain certified confirmation of the document supplied through a person carrying out a relevant financial activity; and (iv) ensure that the first payment or transaction into the account is carried out through an account held in a recognised credit institution.

**d. Outsourcing of identification to third parties**

Regulation 12 provides for instances where a subject person may rely on another subject person or on a third party for the performance of the CDD requirements under the regulations, provided that the relying subject person remains responsible for compliance with the CDD obligations under the regulations. In this regard, the regulations require the relying subject person to ensure that the relevant CDD documentation and information is made available to it.

The regulations provide for third party identification reliance as follows:

- Subject persons as identified under the regulations may rely on other subject persons under the regulations if the latter carry out “relevant financial business” (see “Business Covered By The Legislation” above), or exercise a professional activity as auditors, external accountants, tax advisors, notaries, independent legal professionals, or providers of trustee or any other fiduciary service.
- Subject persons as identified under the regulations may rely on third parties who are situated in another Member State or in a reputable jurisdiction, and who are subject to authorisation to undertake activities equivalent to those falling within the scope of the definition of “relevant financial business”. However, outsourcing to third parties whose main business is currency exchange or money transmission or remittance services is only allowed in the case of subject persons who themselves have, as their main business, currency exchange or money transmission or remittance services.
- Subject persons, as identified under the regulations, who are auditors, external accountants, tax advisors, notaries, independent legal professionals, or persons

providing trustee or any other fiduciary service may rely on third parties (as defined above) who undertake equivalent activities.

**e. Means of identification**

The legislation provides general guidelines on what would constitute adequate evidence of identity.

*Natural persons*

The Regulations require the production of a reliable means of identification but do not establish what specific documents are acceptable. The Guidance Notes have laid down that a national identity card, passport or other document bearing a photograph and other personal details are some of the accepted means of identification.

*Legal persons*

Identification is required for the body corporate, all directors, all qualifying shareholders and all other persons authorised to transact on behalf of the company.

*Natural or legal persons acting for the account of a third person*

Reasonable measures must be taken to establish the identity of all persons concerned, including beneficial owners and qualifying shareholding held under a nominee, trustee or fiduciary arrangement.

**f. Source of information (e.g.: public register for the identification of beneficial owner)**

Corporate ownership structures are validated, as far as practicable, via independent means such as company registry searches, audited accounts, certification by reputable third parties, etc.

Where the tracking of the ownership chain of the principal leads to an entity whose beneficial ownership cannot be traced further (e.g. a foreign-registered company which has bearer shares, or whose shares are held by a nominee), banks normally obtain an auto-declaration of beneficial ownership from the individual(s) who claim(s) to be the owner(s) of such companies. The declaration also incorporates an undertaking by the person(s) signing the declaration to advise the bank of any change in the shareholding position.

## [PRODUCTS AND TRANSACTIONS CHARACTERISED BY A HIGH/LOW RISK OF MONEY LAUNDERING]

### (a) **Low Risk**

- persons authorised to undertake “relevant financial business” (see “Business Covered By The Legislation” above) or equivalent in another Member State or reputable jurisdiction;
- legal persons listed on a locally regulated market or equivalent regulated market within the Community or a reputable jurisdiction;
- beneficial owners of pooled accounts held, for example, by notaries and other independent legal professionals; provided that supporting identification documentation is available or may be made available on request.
- domestic public authorities or public bodies which fulfil certain criteria;
- legal persons which, whilst not having the status of public authorities or public bodies, satisfy certain criteria;
- life insurance policies involving a single premium not exceeding EUR 2,500, or periodic premiums not exceeding €1,000 in any calendar year;
- insurance policies in respect of pension schemes, as well as pension, superannuation or similar schemes that provide retirement benefits to employees;
- electronic money, where the amount that can be stored / recharged, does not exceed €150 or, where a limit of €2,500 *per annum* is imposed for recharging;
- other products which fulfil certain criteria laid down in the Regulations.

### (b) **High Risk**

- where the applicant for business has not been physically present for identification purposes;
- politically exposed persons residing in another Member State or in any other jurisdiction, including their immediate family members or persons known to be their close associates;
- shell banks, with which correspondent banking relationships are prohibited;
- products or transactions that might favour anonymity;
- new or developing technologies which may give rise to the threat of money laundering / funding of terrorism;

- cross-border correspondent banking relationships with respondent institutions from a country other than a Member State.

## [EXISTING GUIDELINES TO THE BANKING INDUSTRY]

Guidance Notes for Credit and Financial Institutions in relation to money laundering were published by the Malta Financial Services Authority in 2003, in consultation with the Financial Intelligence Analysis Unit. These are now being reviewed and updated by the FIAU.

## [GENERAL FEEDBACK (NEW MODUS OPERANDI, TRENDS, REAL CASES, etc)]

According to Article 32 of the Prevention of Money Laundering Act, the FIAU, on the request of a subject person who has filed a suspicious report, shall provide feedback which the FIAU considers to be of interest to that subject person to enable that subject person to regulate its position. The 2008 new regulations further require the FIAU to provide subject persons with timely feedback, on the effectiveness of suspicious transaction reports and other information which it receives, and on the effectiveness of the statistical data gathered.

## [PURPOSES FOR WHICH THE FEEDBACK INFORMATION MAY BE USED]

According to Article 32 of the Prevention of Money Laundering Act, the purpose of the provision of feedback on specific STRs that is provided to the subject person that filed the specific STRs is *in order to enable that subject person to regulate his/her affairs and to assist to carry out duties under this Act or any regulations made hereunder*. Conversely, the provision of general feedback under the new regulations, although not specifically stated under the regulations, is to assist subject persons in understanding possible trends in money laundering or the financing of terrorism, thus enabling them to adjust continuously their preventive internal controls to cater for such developments, and to enable them to understand and measure more efficiently the effectiveness of their role in the chain for the prevention of money laundering and the financing of terrorism.

## [PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK STAFF IN THE EVENT OF NOTIFICATION) OF THE INSTITUTIONS OR PERSONS COVERED BY THIS DIRECTIVE ]

In principle the law requires that any knowledge or suspicion of money laundering / funding of terrorism transactions or any information that could lead to such activities, must be reported.

Any *bona fide* communication or disclosure made in accordance with the Regulations will not be treated as a breach of the duty of professional secrecy, and will not involve the staff and the bank in any liability of any kind.

The Regulations also require any investigating, prosecuting, judicial, or administrative authority and subject persons to protect and keep confidential the identity of persons and employees who report, suspicions of money laundering or the funding of terrorism, either internally or to the FIAU.

## [CONSERVATION OF RECORDS AND DOCUMENTS]

### **(a) Duration**

Identification documents must be kept for at least five years after the relationship with the customer has ended.

Transaction records must be kept for at least five years after the completion of the transaction.

### **(b) Means of conservation**

Unless otherwise provided in other legislation, documents may be kept in formats other than original documents, such as electronic or other forms.

## [STEPS TAKEN TO INCREASE AWARENESS OF THE PHENOMENON OF MONEY LAUNDERING (E.G.: TRAINING, INFORMATION...)]

Institutions run training programmes drawn up for their employees, some of whom are sent on training courses abroad. They also regularly attend and participate in local and international seminars and conferences.

The Malta Bankers' Association together with other recognised associations and bodies representing persons who are subject to the legislation sit on the Joint Committee for the Prevention of Money Laundering and Funding of Terrorism. This Committee is chaired by the FIAU and also includes representatives of supervisory authorities, the Police, and the Attorney General's office. The Committee is not a decision-taking body but provides a forum for discussion and exchange of views relating to the prevention of money laundering and funding of terrorism with a view to developing common standards and best practices.

## THE NETHERLANDS

The Netherlands Bankers' Association

### [ANTI-MONEY LAUNDERING /CTF LEGISLATION]

- 1994: Coming into force of the Disclosure of Unusual Transactions (Financial Services) Act on 1 February 1994.
- 1994: Coming into force of the Identification (Financial Services) Act on February 1994.
- 2002: Implementation of an act making money laundering an autonomous criminal offence.
- 2002: Coming into force of a new Identification Services Act
- 2008: Coming into force of the anti-money laundering and terrorist financing act on 1 August 2008. This law replaces the Compulsory Identification Act (WID) and the Disclosure of Unusual Transactions (Financial Services) Act. It transposes Directive 2005/60/EC and 2006/70/EC.

### [PENALTIES IN NATIONAL LAW FOR FAILURE TO COMPLY WITH THE NATIONAL PROVISIONS OF THE DIRECTIVE]

The Ministry of Finance can impose an administrative fine on institutions that fail to comply with the AML/CFT Act.

### [CENTRAL DISCLOSURE OFFICE]

Banks in The Netherlands have to report unusual transactions to the Financial Intelligence Unit Netherlands (FIU-NL). The FIU is the central agency for the collection and analyses of information needed to detect money laundering and terrorist financing. Operating independently from the police and the judicial authorities, it processes disclosures and, where necessary, conducts further inquiries. If the FIU considers a transaction suspicious, it will forward the information to the appropriate authorities. If the reported transaction is found to be suspicious, the reporting bank will be notified of this.

There is a FIU supervisory committee, which is comprised of representatives of the relevant economic sectors, government officials and regulatory authorities. Its task is to monitor the mandatory disclosure process and the way the FIU performs its duties. In addition, the committee defines the indicators of unusual transactions.

## [PERSONS HANDLING DISCLOSURE]

Within 14 days of detection, an institution is to report the unusual transaction to the FIU. The act does not give any specifications about the internal reporting procedures. In practice, every bank will have a designated officer or unit responsible for the disclosure of unusual transactions.

## [ACTIVITIES COVERED BY THE LEGISLATION (WHICH SPECIFIC PERSONS: NOTARIES, LAWYERS...)]

The act law covers the following institutions:

- Banks and other credit institutions;
- Money service businesses (bureau de change, cheque encashment centre's and money transmission services);
- Life insurance companies;
- Investment companies and institutions;
- Financial service providers (for life insurance);
- Trust service providers;
- Accountants, auditors and tax advisers;
- Lawyers, notaries and other providers of (legal) services that involve participation in a financial or property transaction;
- Dealers in high value goods of any description involving payments of euro 15.000,-- or more;
- Casinos;
- Credit card companies.

## [PREDICATE OFFENCES COVERED]

The law covers the laundering of the proceeds of any type of serious crime and money related to terrorist financing.

Since 2001 money laundering has been criminalized as an autonomous offence.

### **1. Three types of money laundering**

The following three types of money laundering have been included in the Criminal Code since 6 December 2001:

- **Under Section 420bis of the Criminal Code** the intentional type of money laundering is punishable. At the time of the action, the suspect should know that the object he is hiding

or concealing is crime-related. As regards such knowledge, conditional intention shall be sufficient. The terms “hide” and “conceal” used in the description of the offence also imply intent. Here, too, conditional intent shall be sufficient.

- So-called intentional money laundering is the generic term of the special term habitual money laundering, which is punishable under **article 420 of the criminal code**. A person is guilty of habitual money laundering when he repeatedly engages in intentional money laundering.
- Finally, there is the *guilt variant* of money laundering, included in **section 420 quater of the criminal code**. In this latter case it must be proven that the suspect should reasonably have suspected that the object was crime-related. As regards the acts performed by the suspect in respect of the money laundering intent should be proven. Conditional intent is sufficient in this regard; knowingly and willfully exposing oneself to the all but imaginary chance that one’s actions are instrumental in hiding, or concealing, etc., something.

## **2. Independent ground for prosecution**

Before sections 420 bis, 420 ter and 420 quater of the criminal code came into effect, money laundering was considered as a variant of handling stolen goods (section 416 and 417 of the criminal code). However, during the past decade the importance of the independent penalisation of money laundering waws increasingly recognised. Not least of all as a result of the greater importance attached by the policy and the judiciary to the tracing of crime-related money and to dealing with financial facilitators within organised crime (as for instance criminal money exchangers, money couriers, as well as professional service providers).

## **3. No confusion with predicate offence**

Under the money laundering provisions, in order to combat money laundering more effectively, the receiver of stolen goods/stealer rule does not apply, as is the case in sections 416 and 417 of the criminal code. This means that also actions relating to objects originating from crimes committed by the money launderer himself, fall under the provisions of sections 420 bis and 420 ter of the criminal code. This reflects the wish on the part of the legislator to express the independent punishability of money laundering.

It is also important that the Netherlands Supreme Court, in its ruling of 2 October 2007, NJ 2008, 16, determined that the notion that the sole possession of an object is insufficient to qualify same as money laundering, is not supported by law.

## **4. Conviction for predicate offence not requisite**

The money or any other goods that are laundered should proceed from a crime committed prior to that. It is not requisite that the property is wholly crime-related: property that has been financed in part with criminal funds and in part with legal money is regarded as proceeding from crime. It is also important that the Netherlands Supreme Court, in its ruling of 28

September 2004 (LJN No. AP2124, HR 02679/03, determined that proof that the property “proceeds from a punishable fact” does not rest on evidence that the property in question proceeds from an accurately pinpointed crime. This also implies that the evidence does not need to make clear by whom, when and where this crime has actually been committed.

Indeed, nothing appears to stand in the way of also regarding a tax offence as a predicate offence for money laundering.

Besides money laundering, the act also covers the financing of terrorism.

Financing of terrorism is defined as:

- a. the deliberate acquisition or having in possession of goods with a monetary value designed to accommodate the commission of a criminal offence as referred to in section 83 of the criminal code;
- b. the intentional furnishing of monetary resources to accommodate the commission of a criminal offence as referred to in section 83 of the criminal code,
- c. the furnishing of monetary support, as well as the intentional raising of funds for an organisation of which the object is to commit criminal offences as referred to in section 83 of the criminal code.

## [IDENTIFICATION]

### **a) Definition (e.g.: PEPs, beneficial owner, thresholds...)**

#### Politically Exposed Person (PEP)

According to section 8, paragraph 4, an institution has to ensure that it has risk-based procedures in place in order to determine whether the customer is a politically exposed person (PEP) who does not reside in the Netherlands.

It also has to ensure that the decision to enter into a relation is taken by a duly authorised person, that the source of the assets is determined and that the relation is constantly monitored. Based on the directive, PEPs are understood to include, amongst other things: heads of state, government leader, ministers, ambassadors, army officers, etc. Immediate family members (spouse, children, etc.) and close associates of such persons (ultimate beneficiary of a legal entity) are also regarded as PEPs.

Regarding associated persons, the explanatory memorandum to the act notes that an institution is not required to undertake an active investigation into this relation; increased investigation is only necessary if the relation is publicly known.

The principle-based principle enables institutions to determine themselves how the policy regarding PEP is to set up in order to satisfy the legal obligation.

According to the explanatory memorandum, not a single method will be able to prevent that an institutions sometimes fails to (immediately) recognise a PEP as such. Institutions are required, however, to make reasonable efforts to recognise and to identify a PEP.

Guidance Netherlands Bankers' Association

To determine whether a customer is a PEP, the institution can do several things, such as:

- a) Checking public sources (such as the Internet), or
- b) Collecting information from one of its branches in the customer's home country, or
- c) Testing against lists of names furnished by commercial organisations.

## Ultimate Beneficial Owner

An ultimate beneficial owner is defined as:

Any natural person who has sole beneficial ownership of a legal entity or a legal arrangement which is known to have been set up for the benefit de facto of the person referred to in paragraph 1 (see original text of the directive).

To prevent that a legal entity hides individuals who can engage in financial transactions completely anonymously, the Act for the Prevention of Money Laundering and the Financing of Terrorism (WWFT) includes the institution's obligation, where applicable, to identify the ultimate beneficial owner (UBO) and to take risk-based and adequate measures to verify his identity, or where it concerns a legal entity, to take risk-based and adequate measures aimed at gaining insight into the customer's ownership and control structure.

Here, too, the principle-based principle plays an important role. It is up to an institution to determine how the obligation can be met. The only requirement made is that the measures are tailored to the risks involved in respect of the customer, product or transaction in question.

As regards the gaining of insight into the customer's ownership and control structure, an institution need only depend on the information given by the customer (identification) where it concerns a low-risk customer.

With regard to high-risk customers, an institution will be obliged to conduct further investigations, including verification of the information furnished by the customer.

### **b) *Identification threshold amount***

Identification must be verified:

- at the start of a business relation,
- where no continuing business is intended, when the sum involved is 15,000 euros or more,
- whenever money laundering is suspected regardless of the amount, or
- where a money transfer transaction is involved (no threshold amount)

**c) Identification at a distance (non face to face)**

Non face to face is regarded as a high-risk situation. The institutions will then take additional measures to compensate for this. For instance the institution may:

- Verify the customer's identity by means of additional documentation, data or information;
- Verify the documentation furnished by the customer, or
- Check the initial payment from/into the customer's account

**d) Outsourcing of identification to third parties**

Institutions may outsource parts of the customer investigation, including:

- Identification
- UBO identification
- Intended purpose of the relation
- The institution remains responsible
- In case of a structural nature, the agreements are laid down in writing.
- Financial institutions are additionally subject to the outsourcing regime provided for in the Financial Supervision Act (*Wft*)

**e) Means of identification**

Dutch law draws a clear distinction between:

Identification = causing a person to state his identity

Verification = identifying a person by means of documents, etc.

Verification

- *Natural persons:*
  - Documents, particulars or information obtained from a reliable source
  - Documents referred to in a ministerial regulation
- *Dutch legal entity*
  - Documents, particulars or information obtained from a reliable source
  - Documents referred to in a ministerial regulation
- *Foreign Legal entity*
  - Reliable documentation conventionally used in cross-border transactions. Or designated under domestic law
- *Other institutions (religious bodies, owners associations (VvE) etc.):*
  - By ministerial regulation

**f) Source of information (e.g.: public register for the identification of beneficial owner)**

The chamber of commerce can be checked (for legal persons). In the Netherlands registration in the trade register is compulsory for every company and almost every legal entity. There is no such thing as public register for the identification of beneficial owners.

[PRODUCTS AND TRANSACTIONS CHARACTERISED BY A HIGH/LOW RISK OF MONEY LAUNDERING]

**Low risk:**

If the customer is:

- A financial institution established in the EU and certain other countries with similar regulations and supervision (designated by the minister)
- Listed companies in member states and certain other countries
- Customers keeping money on accounts of notaries and lawyers
- A Dutch government body
- A European body
- No customer investigation will be required (unless there is a money-laundering risk)
- Furthermore, there will be a low risk customer investigation in case of:
  - Life Assurance policy with a contribution of less than EUR 1,000 a year or a lump sum of EUR 2,500.
  - Pension Insurance contract, without surrender clause
  - Electronic money (to a limited amount)
  - Prepaid cards of EUR 50. or electronic systems (up to EUR 2,500 a year)

**High risk**

- If risk of money laundering or terrorist financing is high
- In case of non face to face contact
- In case of a correspondent bank relation with a bank established in a non EU member state
- If the customer is a PEP

## [EXISTING GUIDELINES FOR THE BANKING INDUSTRY]

The Netherlands Bankers Association (NVB) has formulated general guidelines with respect to the list of AML/CFT indicators.

At the beginning of 2009, guidance will be given by the NVB about the risk-based possibilities of implementing the new AML/CFT act.

## [GENERAL FEEDBACK (NEW MODUS OPERANDI, TRENDS, REAL CASES, etc)]

In order to satisfy the legal requirements to inform reporting entities about the follow-up to the disclosures, feedback is given in five different ways:

- Individual feedback: acknowledgement of receipt
- Individual feedback: forwarding to “suspicious”
- Individual feedback: outcome report
- General feedback: statistical analysis of forwarded disclosures
- General feedback : case histories, typologies, trends

### Individual: acknowledgement of receipt

Upon each disclosure all reporting entities will receive acknowledgement from FIU-Nederland that the report has been received. This currently happens five days after the disclosure was received by the reporting office. The acknowledgement of receipt lists the transaction number, the recording date and the so-called guide list number, which is used for internal registration purposes. In some cases the acknowledgement of receipt is sent in batches. The acknowledgement of receipt is important in that it holds the reporting entities harmless.

### Individual feedback: forwarding to “suspicious”

This kind of feedback will be subject to the condition that the feedback to the reporting entity can be delivered to a central department with an independent function (e.g. a compliance department). Such an independent department does not maintain relations with customers and does not share the information on forwarded reports to “suspicious” with any other sections of the institution.

## Individual feedback: outcome report

The new act, as in fact does the current act, specifically provides for feedback in the form of outcome reports.

According to the explanatory memorandum, the proposal means that reporting entities must receive an outcome report that, in case of a transaction that is declared suspicious, outlines the outcome of a subsequent criminal investigation. Article 391 of the Criminal Records Act (*Wet Justitiële en strafvorderlijke gegevens*) provides in what circumstances the Board of Procurators General is allowed to furnish data on criminal proceedings. In accordance with this act the Board will be asked for advice on the further elaboration of the outcome reports.

## General statistical analysis of forwarded reports

In accordance with evaluation criteria of the FATF, the FIU will annually furnish reporting entities with an analysis of the reports, broken down by reason for forwarding, type of indicator, time at which the original report has come in or any other characteristics. Furthermore, the FIU annually puts out, for each reporting group or professional group, detailed case histories that have proven valuable. Performance agreements about this obligation are being made with the public prosecutor and the departments involved.

## General case and histories, typologies, trends

The FIU the public prosecutor inform the reporting entities by means of the website, through newsletters and through the organisation of “reporting entities days” about trends that have been found important for the investigation services. Communication with the reporting entities is also important for the FIU and the public prosecutor to keep abreast of new developments with regard to money laundering practices.

The responsible Ministries of Finance and Justice, in turn, will make a contribution through the Working Group for Indicators. In this working group the reporting entities, the regulators the FIU and the public prosecutor present their analyses of trends, typologies, and case histories with regard to money laundering and the financing of terrorism. The sharing of information in this working group can serve as input for the periodic updating of the guidelines.

## [PURPOSES FOR WHICH THE FEEDBACK INFORMATION MAY BE USED]

The purpose of receiving general feedback is that the descriptions of characteristics and trends produce an up-to-date idea of the risks. General feedback must make a real contribution to the ability to recognise money laundering activities.

This will enable the institution to adapt its monitoring systems accordingly and will keep the staff alert (training and information).

The purpose of the individual feedback is that the reporting entity can use it to tailor its own position vis-à-vis the customer and his transactions and thus avoid integrity risks. Based on the internal reports, in relation to the feedback, the reporting entities must be able to assess whether and if so, to what extent further investigation is necessary. This assessment also involves an enhanced investigative focus on certain accounts and/or transactions.

## [PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK STAFF IN THE EVENT OF DISCLOSURE) OF THE INSTITUTIONS OR PERSONS COVERED BY THIS DIRECTIVE ]

Under the AML/CFT act the institution is liable under criminal law. Violation of the regulations would mean that the legal entity, not the individual employee, is liable.

Money laundering and accommodating such practice is punishable by law. Still, the act rules out that an institution that has made a disclosure based on these details is convicted. This indemnity relates to the information reported by the institution only. The indemnity covers both the institutions and their staff insofar as they are involved in the disclosure.

Besides this indemnity against criminal proceedings, there is also indemnity against civil proceedings. The latter implies that the institution (and employee) cannot be held liable for any damage sustained by a third party as a result of a disclosure. The indemnity against liability does not apply if it is proven that, in view of all the facts and circumstances, disclosure should, in all reasonableness, not have been made.

## [PRESERVATION OF RECORDS AND DOCUMENTS]

After verification the institution must record the identity in an accessible manner the following particulars.

### ***Natural persons:***

- Name, date of birth, address and place of residence or establishment of the customer.
- Nature, number and date and place of issue of the identity document
- Nature of the service

### ***Legal persons:***

- Legal form, name given in the articles of association, business name, address and Chamber of Commerce and number, if applicable.

- Name and date of birth of the representative
- Nature of the service.

The institution must preserve the data in an accessible manner for a period of five years of the date of the termination of the business relation or up to five years of the date of execution of the transaction in question

Other statutory provisions may make longer storage periods compulsory.

The disclosure details relating to an unusual transaction must also be preserved for a period of five years.

[STEPS TAKEN TO INCREASE AWARENESS OF THE PRACTICE OF MONEY LAUNDERING  
(E.G.: TRAINING, INFORMATION...)]

Under the act, an institution must ensure that its employees, insofar as relevant to the exercise of their duties, are cognisant of the legal regulations and are trained to recognise unusual transactions.

To achieve this, the banks develop different instruments (including e-learning or in-company training).

## NORWAY

Norwegian Financial Services Association

*NB: The Norwegian Government is currently incorporating the Third Anti Money Laundering Directive (2005/60/EC), which is expected to pass Parliament in February 2009 and enter into force during summer 2009. No regulation is adopted yet and no translation is consequently available. The new General Penal Code is also expected to pass Parliament this spring.*

*This review is partly based on existing legislation, but mostly on the proposal for new legislation and regulation.*

### [ANTI-MONEY LAUNDERING /CTF LEGISLATION]

- The General civil penal code of 1902 Section 317 on receiving the proceeds of a criminal act
- The General civil penal code of 1902 Section 147 a, Section 147b and 147 c on terrorism

The proposal for a new General penal code of 2005 new Section 337 Money laundering and new Section 337 Severe Money laundering, is expected to be enacted by the Parliament in February/March 2009. Chapter 18 on terrorism is enacted, but have not yet entered into force.

- Act of 20 June 2003 No 41 on measures to combat the laundering of proceeds etc

The Parliament is expected to enact a new bill in February 2009 in order to be compliant with 3<sup>rd</sup> directive, and the new anti money laundering legislation is expected to enter into force by summer 2009.

- Regulation 10 December 2003 No. 1487 on measures to combat the laundering of proceeds of crime etc. (Money Laundering Regulations)

The regulation is expected to be replaced in spring 2009 in order to be compliant with 3<sup>rd</sup> directive.

The answers below are to be regarded as a preliminary short version until an official translation is made available. The answers are based on the current proposal for a new act on money laundering by the Ministry of Finance and a proposal for a new Penal Code by the Ministry of Justice.

## [PENALTIES IN NATIONAL LAW FOR FAILURE TO RESPECT OF THE NATIONAL PROVISIONS TO THE DIRECTIVE]

The new anti-money laundering act section 28 states that any who fails to comply with section 5, 6, 7, 8, 15, 17, 18 or 22 or regulation pursuant these sections can be liable to penalties such as a fine or in severe cases prison for up to one year.

## [CENTRAL AUTHORITY FOR REPORTING]

Norway's financial intelligence unit (FIU) is named Økokrim. The Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim) was established in 1989 and is both a national police unit and a prosecution authority. Økokrim is organised with multidisciplinary teams. One of ØKOKRIM's tasks is to receive and process suspicious transaction reports pursuant to the Money Laundering Act. As a police agency, ØKOKRIM reports to the National Police Directorate regarding administration and funding. When it comes to prosecution of criminal cases, ØKOKRIM reports to the Director General of Public Prosecutions. They all report to the Ministry of Justice.

## [PERSONS RESPONSIBLE FOR REPORTING]

A person in the management shall be assigned special responsibility for following up the procedures, according to the proposal for a new Act Section 23.

## [BUSINESS COVERED BY THE LEGISLATION (WHICH SPECIFIC PERSONS: NOTARIES, LAWYERS...)]

According to Section 4 in the proposal for a new Act "Scope of Application", the Act applies to the following undertakings and legal persons:

- (1) financial institutions,
- (2) Norges Bank (Central Bank of Norway),
- (3) e-money institutions,
- (4) institutions operating activities consisting of transfer of money or financial claims,
- (5) investment firms,
- (6) management companies for securities funds,
- (7) insurance companies,

- (8) insurance brokers,
- (9) postal operators in connection with provision of postal services,
- (10) securities registers,
- (11) services associated with letting of safe deposit boxes

The Act also applies to the following legal and natural persons in the exercise of their professions:

- (1) state authorised and registered public accountants,
- (2) authorised external accountants,
- (3) lawyers and other persons who provide independent legal assistance on a professional or regular basis when they assist or act on behalf of clients in planning or carrying out financial transactions or such transactions concerning real property or movable property of NOK 40 000 or more ,
- (4) real estate agents and housing associations that act as real estate agents,
- (5) companies who provide services similar to those listed above from No 4 to No. 5
- (6) corporate services providers (establishing of businesses etc.),
- (7) dealers in objects, including auctioneering firms, commission agents and the like, in connection with cash transactions of NOK 40 000 or more or a corresponding amount in foreign currency.

This Act also applies to persons and undertakings who perform services on behalf of or for entities with a reporting obligation.

When a lawyer acts as manager of a bankrupt's estate, the provisions laid down in sections 17, 18, 20, 21, 27 and 28 shall apply.

The King may in regulations lay down provisions concerning the application of this Act.

## [PREDICATE OFFENCES COVERED]

In principal all predicate offenses are covered according to a change in the General Civil Penal Code of 1902, which will be continued in the new Penal Code of 2005 not yet entered into force.

## [IDENTIFICATION]

### **a. Definition (e.g.: PEPs, beneficial owner, thresholds...)**

The new Act Section 2 contain definitions of transaction, beneficial owner  
The new Regulation Section 9 contain a definition of PEPs

### **b. Identification threshold amount**

According to the new Act Section 6, the client must be identified if a customer relationship is established, or if he carries out a transaction of more than approximately 11.000 euro, or if a suspicious situation had occurred.

### **c. Identification at a distance (non-face to face)**

According to the new Act Section 7 forth sentence, further documentation on identity must be submitted.

### **d. Outsourcing of identification to third parties**

An entity with a reporting obligation may, pursuant to the new Act Section 12 enter into a written agreement with another entity with a reporting obligation or post office with a license regarding verification of identity that entities with a reporting obligation are obliged to perform. In such cases the primary entity with a reporting obligation is responsible for ensuring that identity verification is carried out in due and proper manner in accordance with law and regulations and for establishing proper routines.

### **e. Means of identification**

Natural persons, physical ID: According to the new Regulation Section 4 a identification document must be issued by a public administration or another body with proper control routines for issuing of IDs with satisfactory safety level, and include full name, signature, photo and birth number or an equal number.

Natural persons, electronic ID: According to Section 5 it must be issued according to Regulation 21 November 2005 No. 1296 Section 3.

Legal persons: According to Section 6 a registration certificate not older than three months is regarded as a valid ID.

**f. Source of information (e.g.: public register for the identification of beneficial owner)**

No public register are available for identification of beneficial owner.

[PRODUCTS AND TRANSACTIONS CHARACTERISED BY A HIGH/LOW RISK OF MONEY LAUNDERING]

According to Section 10 in the proposal for a new Regulation “Investigation of suspicious transactions”; examples of circumstances that may trigger the obligation to make investigations are that the transaction (1) appears to lack a legitimate purpose, (2) is unusually large or complex, (3) is unusual in relation to the customer's habitual business or personal transactions, (4) involves a transfer to or from a customer in a country or area lacking satisfactory measures against money laundering or terrorist financing, or (5) is otherwise of an anomalous nature.

[EXISTING GUIDELINES TO THE BANKING INDUSTRY]

The Financial Supervisory Authority of Norway published general guidelines for all private entities covered by the anti money laundering legislation, including banks in 2004, which is to be replaced soon according to the provisions in EU3 and the new Norwegian act and Regulation. On the Norwegian banking association homepage <http://www.fnh.no> there are also a set of guidelines (in Norwegian language only) on identity check containing recommendations for establishing of customer relationships, handling of transactions with customers without a previous relationship, recommendations regarding identity papers, and recommendations for handling of typical special suspicious customers and transactions.

[GENERAL FEEDBACK (NEW MODUS OPERANDI, TRENDS, REAL CASES, etc)]

FIU (Økokrim) submit only general feedback on modus operandi etc. Official reports indicate that the content of the suspicious transactions (STRs) can be linked to different types of crime. *Modus operandi* indicates the type of crime the FIU believes STRs can be related to. Based on reports so far, FIU in Norway estimates that tax evasion constitutes almost 40%, and fraud at least 15% of the reported transactions, while possible terrorist financing constitute only 3%.

[PURPOSES FOR WHICH THE FEEDBACK INFORMATION MAY BE USED]

According to Section 29 in the proposal for a new Act, The Ministry of Finance may lay down regulations regarding the handling of suspicious transactions. The information is only used in criminal investigations. ØKOKRIM may provide information that it receives pursuant to the

provisions of section 18 to public authorities other than the police that are engaged in tasks associated with the prevention of offences covered by section 147a, section 147b or section 147c of the Penal Code (terrorist financing etc.).

## [PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK STAFF IN THE EVENT OF NOTIFICATION) OF THE INSTITUTIONS OR PERSONS COVERED BY THIS DIRECTIVE ]

According to Section 28 in the proposal for a new Act, entities or individuals that wilfully or by gross negligence contravene or are accessory to any contravention of this Act Section 5, 6, 7, 8, 15, 17, 18, eller 22, or regulations laid down pursuant thereto shall be liable to fines. In the case of particularly aggravating circumstances, imprisonment for a term not exceeding one year may be imposed.

According to Section 20 in the proposal for a new Act, information provided to FIU in good faith pursuant to section 18 does not constitute a breach of the duty of secrecy and does not provide a basis for compensation or penalties.

According to Section 21 in the proposal for a new Act, neither the customer nor any third party shall be made aware that investigations as mentioned above are being carried out. Certain exceptions are laid down in the proposal for a Regulation Section 12. Further protection measures are not yet established.

## [CONSERVATION OF RECORDS AND DOCUMENTS]

According to Section 22 of the new Act, the entity with a reporting obligation shall retain a copy of the necessary documents used in connection with proof of identity and data recorded for five years after termination of the customer relationship or after the transaction is carried out. Documents and other data retained by the entity with a reporting obligation shall be destroyed within one year after expiry of the retention period.

According to Section 15 of the proposal for a new Regulation, data as mentioned shall be retained in the form of copies of presented identity documents. Each copy shall be endorsed with "certified true copy" and the signature of the person who carried out the verification of identity. Entities with a reporting obligation shall retain data by such means as ensure that the documents do not lose their value as evidence.

Entities with a reporting obligation shall ensure that documents are secured so as to protect them against unauthorised access. Act relating to the Processing of Personal Data (Personal Data Act), with appurtenant regulations, applies to the retention of personal data by entities with a reporting obligation.

[STEPS TAKEN TO INCREASE AWARENESS OF THE PHENOMENON OF MONEY LAUNDERING (E.G.: TRAINING, INFORMATION...)]

According to Section 23 of the proposal for a new Act, entities with a reporting obligation shall establish satisfactory internal control and communication procedures Training program and follow up, shall be implemented for employees and other persons who perform tasks in fulfillment of obligations, pursuant to the Act.

The obligations also include measures such as training, maintenance and upgrading of expertise, including participation in special training program in which employees and other persons who perform tasks in fulfillment of the regulations learn to recognise transactions which may be related to the laundering of proceeds of crime, and receive instruction in handling such a case.

### ANTI MONEY LAUNDERING /CTF LEGISLATION

- The Banking Act of 29 August 1997 - Journal of Laws of 2002 No. 72 item 665 with later amendments;
- The Act on counteracting the introduction into financial turnover of assets originating from illegal or undisclosed sources and counteracting the terrorism financing of 16 November 2000, Journal of Laws of 2003 No. 153 item 1505 with later amendments;
- Ordinance of Minister of Finance of 20 May 2003 on the definition of transaction register template, the mode of its maintenance and the mode of submitting the data from the register to the General Inspector of Financial Information – Journal of Laws of 2003 No. 101 item 935;
- The Penal Code of 6 June 1997 - Journal of Laws of 1997 No. 88 item 553 with later amendments;
- The Act on public trading in Securities of 29 September 2005 – Journal of Laws of 2005 No. 183 item 1538 with later amendments.

### [PENALTIES IN NATIONAL LAW FOR FAILURE TO RESPECT OF THE NATIONAL PROVISIONS TO THE DIRECTIVE]

Penalties are imposed by both *The Act on counteracting the introduction into financial turnover of assets originating from illegal or undisclosed sources and counteracting the terrorism financing of 16 November 2000 - Chapter 8* and *The Penal Code of 6 June 1997 Art. 299*;

Any person committing a crime of “money laundering” described in Art 299 of the Penal Code shall be liable to a penalty of deprivation of liberty for a period of 6 months to 8 years (and up to 10 years in case of organized crime);

Any person acting in the name or in the interest of an obligated institution who violates the Act, shall be liable to a penalty of deprivation of liberty for a period of three months to five years.

### [CENTRAL AUTHORITY FOR REPORTING]

The *General Inspector of Financial Information (GIFI)*, in the rank of the Undersecretary of State at the Ministry of Finance. The General Inspector of Financial Information governs the unit being a part of the Ministry of Finances.

All transactions over €15.000 and all suspicious transactions irrespectively of their value have to be reported to GIFL.

GIFL has a right to stop a transaction and/or block an account for 48 hours as well as report the transactions and other related data to Prosecutor Office or other Law Enforcement Agencies.

## [PERSONS RESPONSIBLE FOR REPORTING]

Management of each “obliged” institution has to set up suitable money laundering prevention procedures and appoint a person responsible for preparing and putting into operation such procedures.

All customer identification data and information on the money laundering prevention procedures must be disclosed to the authorized employees of the General Inspectorate of Financial Information and within the legal proceeding to the Prosecutor or Court. The bank’s information related to AML would be also accessible to the authorized staff of the General Inspectorate of Banking Supervision.

## BUSINESS COVERED BY THE LEGISLATION (WITH SPECIFIC PERSONS: NOTARIES, LAWYERS)

- Penal Code has general application;
- Banking Law applies to banks and credit institutions;
- Public Trading in Securities Act covers brokerage houses;
- The Act on counteracting the introduction into financial turnover of assets originating from illegal or undisclosed sources and counteracting the terrorism financing defines a large number of “obliged institutions”: banks, brokerage houses, notaries, real estate, agencies, casinos, Post Office, leasing companies, pension funds, legal advisors, etc. These entities must monitor their financial operations and report suspicious transactions to the GIFL.

## [PREDICATE OFFENCES COVERED]

Any form of serious crime, *inter alia*:

- trafficking in arms and nuclear materials;
- drug – related offences;
- forgery of currencies and securities;
- extortion;
- armed robbery;
- smuggling;

- terrorism.

and tax evasion, duty and obligatory social insurance payments.

#### [IDENTIFICATION]

##### **a. Definition (e.g.: PEPs, beneficial owner, thresholds...)**

Obligated institutions have to identify their clients whenever they receive from them instruction or order to execute a transaction. The identification requirement shall extend also to beneficiaries of the transaction and include the determination and noting their name (firm) or first name, last name and address, in the extent possible to determinate by the obligated institution performing with due diligence

If circumstances of the transaction suggest that the person executing it does not act in her/his own name, the obligated institution should try to identify the entities, in the name or on behalf of which, the person executing the transaction is acting.

PEP and UBO (Ultimate Beneficial Owners) are not defined in Polish legislation.

##### **b. Identification threshold amount**

Customers must always be identified when the transaction exceeds the equivalent of € 15,000 or when the transaction is suspicious.

##### **c. Identification at a distance (non face to face)**

Banks are obliged to verify the clients' identity with valid ID documents. Generally, such a verification is based on face-to-face procedure although in some financial institutions that are obliged to report suspicious transactions, distance identification procedures with the use of an electronic signature are allowed as regulated by the Electronic Signature Act.

At the request of the Banks Supervisory Body, the banks are to implement the identification standards in line with the Basel Committee requirements.

##### **d. Outsourcing of identification to third parties**

There are no detailed regulations regarding outsourcing of identification to third parties. General outsourcing requirements are regulated by the Banking Act.

**e. Means of identification**

- Natural persons: determining and noting the distinguishing features of a document confirming the person's identity pursuant to separate regulations, or of a passport, as well as the first name, last name, the citizenship and address of the person executing the transaction, and furthermore, the PESEL (national citizens' registry) number in case of the identification on the base of identity card or country code in case of the passport.
- Legal persons: noting of up-to-date information from a court registry extract or some other document specifying the name (firm), the organizational form of the legal entity, its seat and address, and information from a valid document confirming the authority of the person executing the transaction to represent the legal entity, as well as noting of data described above pertaining to the representing person;

Natural or legal persons acting for the account of a third person: after identification of the person who is physically undertaking the transaction, the proxy must disclose the identity of the persons on whose behalf the operation is being made.

**f. Source of information (e.g.: public register for the identification of beneficial owner)**

Obligated institutions do not have an access to any special databases e.g. databases of national id numbers (PESEL). They can only use public registers like *Court register of companies*.

**PRODUCTS AND TRANSACTIONS CHARACTERISED BY A HIGH/LOW RISK OF MONEY LAUNDERING**

There is no reference to product/transaction characterized by high/low risk of money laundering in Polish legislation.

**[EXISTING GUIDELINES TO THE BANKING INDUSTRY]**

GIFI issued a dedicated *Guidance for obliged institutions and co-operating units* covering wide range of AML issues e.g. some theory followed by examples describing typical *modus operandi* and obligations.

## GENERAL FEEDBACK (NEW MODUS OPERANDI, TRENDS, REAL CASES, etc)

GIFI publicises on official government web site <http://www.mofnet.gov.pl> general reports of its activity, frequently ask questions, and important news.

However, there are no provisions for feedback from GIFI following notification of a suspicious operation.

## PURPOSES FOR WHICH THE FEEDBACK INFORMATION MAY BE USED

The general information can be used by obliged institutions to support their AML activity

## PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK IN THE EVENT OF NOTIFICATION) OF THE INSTITUTIONS OR PERSONS COVERED BY THE DIRECTIVE

Any person reporting facts to the appropriate authority, suggesting criminal offences, or any such report -unless it has been made untruthfully with the intent to mislead, or unless there has been gross negligence -cannot be held liable.

## [CONSERVATION OF RECORDS AND DOCUMENTS]

### **a) Duration**

Identification records and documents must be kept for 5 years.

### **b) Means of conservation**

Original paper and/or microfilm/electronic form.

## STEPS TAKEN TO INCREASE AWARENESS OF THE PHENOMENON OF MONEY LAUNDERING (E.G.: TRAINING, INFORMATION)

The General Inspector of Financial Information introduced an AML awareness programme and a set of training for the obliged institutions. The Polish Bank Association organizes seminars on the subject of money laundering and bank fraud. All obliged institutions are obliged to provide the AML internal staff training.

## PORTUGAL

Portuguese Banking Association

### [ANTI-MONEY LAUNDERING /CTF LEGISLATION]

Law n° 25/08, of 5 June 2008, which transposes the third AML Directive into the Portuguese Law, consolidates all provisions and replaces the former legislation.

### [PENALTIES IN NATIONAL LAW FOR FAILURE TO RESPECT THE NATIONAL PROVISIONS TO THE DIRECTIVE]

Regarding financial institutions: a fine of €25.000,00 to €2.500.000,00 for legal persons and of €12.500,00 to €1.250.000,00 for natural persons.

Regarding non-financial institutions: a fine of €5.000,00 to €500.000,00 for legal persons and of €2.500,00 to €250.000,00 for natural persons.

### [CENTRAL AUTHORITY FOR REPORTING]

The Prosecutor General and the Financial Intelligence Unit (FIU).

### [PERSONS RESPONSIBLE FOR REPORTING]

Regarding financial institutions, the Compliance Head Officer or the person in charge of internal audit.

Regarding non-financial institutions, the executives of the company concerned.

### [BUSINESS COVERED BY THE LEGISLATION (WHICH SPECIFIC PERSONS: NOTARIES, LAWYERS...)]

The law covers financial institutions, i.e.:

- Credit institutions and financial institutions (both those with their head office in Portugal and branches located in Portugal which have their head office elsewhere);
- Finance companies;

- Life insurance companies;
- Pension fund management companies;
- Post banks;
- Securitization companies;
- Foreign exchange offices;
- Investment funds management companies.

The law also covers non-financial institutions, including:

- Casinos;
- Estate agents;
- Real-estate management companies;
- Companies which organise gambling or lotteries;
- Dealers in antiques or works of art;
- Jewellers;
- Aircraft, boat and car dealers;
- Auditors and external accountants;
- Cash and value carriers;
- Notaries and registry officers;
- Lawyers (barristers and solicitors);
- Tax advisers.

## [PREDICATE OFFENCES COVERED]

The offences covered are those relating to drug trafficking, terrorism, arms, and nuclear devices trafficking, extortion, kidnapping, procuring, human organs' trafficking, child pornography, corruption, economic and financial crimes, tax fraud and, in general, any offence punishable by a sentence of imprisonment of a minimum of more than 6 months and of a maximum of more than 5 years.

## [IDENTIFICATION]

### **a. Definition (e.g.: PEPs, beneficial owner, thresholds...)**

The definitions of PEPs and beneficial owner are the same as those of the Directive.

**b. Identification threshold amount**

- For banks and other financial institutions: customers must be identified when they initiate operations for amounts in excess of € 15.000,00
- For non-financial institutions, the identification thresholds are the following:
  - casinos: €2.000,00 for each transaction;
  - antiques and art dealers, jewellers, aircraft, boat and car dealers: €15.000,00 for each cash transaction;
  - gambling or lottery companies: €5.000, 00 for each transaction;
- estate agents and real-estate management companies: they must always identify their customers.

**c. Identification at a distance (non face to face)**

The measures of our law are the same as those of the Directive.

**d. Outsourcing of identification to third parties**

This is permitted to financial institutions, but not to currency exchange offices. The third party must be a financial institution established in Portugal, in another Member State or in a third equivalent country.

**e. Means of identification**

Customer identification must be made by a valid probative document, containing a photo which indicates the complete name, the date of birth, and the nationality of the person concerned.

Current means of customer identification are the following:

**Natural persons:**

- Portuguese citizen: national identity card;
- Foreign residents: residence permit;
- Non-EC residents: passport;
- EC residents: national identity card or passport

**Natural or legal persons acting for the account of a third person:**

- Natural person: the identity card of the person holding the power of attorney and of the third party, together with the power of attorney itself;
- Legal person: the corporate registration card of the legal person holding the power of attorney and the power of attorney itself.

**f. Source of information (e.g.: public register for the identification of beneficial owner)**

The client's declaration and the public registers for the identification of the beneficial owner.

[PRODUCTS AND TRANSACTIONS CHARACTERISED BY A HIGH/LOW RISK OF MONEY LAUNDERING]

Our law contains a provision similar to article 8.2. of the Directive, but there is no list of products or transactions characterised by high or low risk.

[EXISTING GUIDELINES TO THE BANKING INDUSTRY]

Our Central Bank will issue a Regulation by the end of this year.

[GENERAL FEEDBACK (NEW MODUS OPERANDI, TRENDS, REAL CASES, etc)]

Our Central Bank and FIU issue regular information on the practices of the money launderers and terrorist financiers and our FIU gives feed-back on the outcome of the disclosures.

[PURPOSES FOR WHICH THE FEEDBACK INFORMATION MAY BE USED]

Only by the institution that has reported the suspicious operation, to prevent similar situations and to motivate the personnel that made possible the disclosure.

[PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK STAFF IN THE EVENT OF NOTIFICATION) OF THE INSTITUTIONS OR PERSONS COVERED BY THIS DIRECTIVE ]

The identity of the employees or the persons covered by the Directive can never be revealed.

[CONSERVATION OF RECORDS AND DOCUMENTS]

Records and documents must be kept for a period of seven years.

[STEPS TAKEN TO INCREASE AWARENESS OF THE PHENOMENON OF MONEY LAUNDERING (E.G.: TRAINING, INFORMATION...)]

Several training sessions have been held and are still under way, either within each bank or at sectoral level.

### [ANTI-MONEY LAUNDERING /CTF LEGISLATION]

Slovak Parliament has adopted new AML Act as a harmonisation of 3rd AML Directive . Act No. 297/2008 Coll on the Prevention of Legalization of Proceeds of Criminal activity and Terrorist Financing. This act came into effect on 1 September 2008.

### [PENALTIES IN NATIONAL LAW FOR FAILURE TO RESPECT OF THE NATIONAL PROVISIONS TO THE DIRECTIVE]

Penalties in volume up to 10.000.000,-SKK (332 000 EUR) and/or revocation of licence for conducting business.

### [CENTRAL AUTHORITY FOR REPORTING]

The Financial Intelligence Unit shall serve as a national unit for the area of the prevention and detection of legalization and terrorist financing. The Financial Intelligence Unit shall (among other activities):

- a) receive, analyze, evaluate and process unusual transaction reports and other information related to legalization or terrorist financing for the fulfilling the tasks under this Act or under a special regulation,
- b) submit a case to law enforcement authorities if the facts indicate that a crime has been committed,
- c) require and control the compliance to obligations by obliged entities stipulated by this Act,
- d) submit initiative for imposition of a fine on an obliged entity due to infringement or non-performance of obligations with an authority which is under a special regulation authorized to fine the legal entity, unless that authority itself deals with the case under Sec. 32 or 33,
- e) submit initiative for revocation of an obliged entity's licence for the conduct of business or other independent gainful/profitable activity of the obliged entity due to repeated infringement or non-performance of obligations stipulated by this Act with an authority which is authorized to decide on the revocation of the licence under a special regulation

- f) require that the authorities with which a proposal for imposition of a fine or a initiative for revocation of a licence has been filed give notification/feedback on the way of handling the proposals and initiatives submitted and on the measures adopted.

[PERSONS RESPONSIBLE FOR REPORTING]

## Contact Person

Obligated entity shall be obliged to prepare an activity programme aimed at the prevention of legalization and terrorist financing (hereinafter referred to as the “Programme”). Programme shall contain appointment of a person who is liable for the prevention of legalization and terrorist financing and provides reporting of unusual transactions and ongoing contact with the Financial Intelligence.

[BUSINESS COVERED BY THE LEGISLATION (WHICH SPECIFIC PERSONS: NOTARIES, LAWYERS...)]

### (1) Obligated entity for the purposes of this Act understood

- a. a credit institution
- b. a financial institution other than a credit institution, such as the Central Securities Depository, a stock exchange, a commodity exchange, an asset management company and depository, a securities dealer, an investment services broker, a foreign collective investment entity, an insurance or re-insurance company, an insurance broker and a reinsurance broker, a pension asset management company, a supplementary pension insurance company, a legal person or a natural person authorized to perform exchange of foreign currency or wireless foreign currency transfers, or to provide foreign exchange services, a legal person or a natural person authorized to trade in receivables a legal person or a natural person authorized to carry out auctions safe for distraintments, finance lease or other financial services pursuant to a special regulation,
  - a. the Export-Import Bank of the Slovak Republic,
  - b. a gambling game operator,
  - c. a postal undertaking,
  - d. a court distrainer,
  - e. an administrator who manages in bankruptcy, restructuring or debt removal proceedings under a special regulation,
  - f. an auditor, an accountant, and a tax advisor,
  - g. a legal person or a natural person authorized to perform real estate brokerage services,

- h. an advocate or notary who provides the customer with services related to
  - purchase or sale of real estate or ownership interests in a company,
  - management or safekeeping of funds, securities or other property,

(2) Opening or management of an account with a bank or a foreign bank branch or of a securities account, or

(3) Establishment, operations or management of a company, an association of a natural person or a legal persons, a special-purpose corporation or another legal entity,

- k) a company service provider, unless it is an obliged entity referred to at letter h) or j),
- l) a legal person or a natural person authorized to provide the services of corporate or economic advisors, the services of public carriers or messengers or forwarding services,
- m) a legal person or a natural person authorized to operate an auction hall, a legal or natural person authorized to trade in works of art, collector's items, antiques, cultural monuments, items of cultural heritage, precious metals or gemstones, a legal or natural person authorized to place products made of precious metals or gemstones on the market, or a legal or natural person authorized to operate a pawnshop,
- n) a legal person or a natural person authorized to mediate housing savings,
- o) other person if so stipulated by a special regulation.

(4) For the purposes of this Act, obliged entity shall also mean a branch, a business unit or establishment of a foreign legal person or a natural person referred to in subsection 1, including an agency of a foreign credit institution or a foreign financial institution, which operate in the Slovak Republic.

(5) For the purposes of this Act, obliged entity shall also mean an entrepreneur not referred to in subsections 1 and 2, who carries out cash transactions in the amount of EUR 15,000 or more, regardless of whether the transaction is carried out in a single operation or in several operations which appear to be linked.

[IDENTIFICATION]

**a. Definition**

**PEP:**

(1) Politically exposed person for the purposes of this Act shall be understood a natural person who is entrusted with prominent public functions who having not permanent residence in the Slovak Republic during and one year after his term of office.

(2) Prominent public office shall mean:

- a) head of state, prime minister, deputy prime minister, minister, head of a government agency, state secretary or a similar deputy of a minister;
- b) member of Parliament;
- c) judge of the supreme court, judge of the constitutional court or other high-level judicial body the decisions of which are not subject to further appeal, except in exceptional circumstances;
- d) member of the court of auditors or of the central bank board;
- e) ambassador or chargé d'affaires;
- f) high-rank military officer;
- g) member of executive body or supervisory body of a state enterprise or a state-owned company; or
- h) a person holding a similar post in the institutions of the European Union or international organizations.

(3) Politically exposed person for the purposes of this Act shall also be understood a natural person who is

- a) spouse, or partner equivalent to spouse, of a person referred to in subsection 1,
- b) child, son-in law or daughter-in law of a person referred to in subsection 1, or a person having a status similar to that of son-in law or daughter-in law of a person referred to in subsection 1; or
- c) parent of a person referred to in subsection 1.

(4) Politically exposed person for the purposes of this Act shall also be understood a natural person to be beneficial owner of

- a) the same customer, or to be otherwise in control of the same customer, as a person referred to in subsection 1, or runs a common business with a person referred to in subsection 1; or
- b) a customer established for the benefit of a person referred to in subsection 1.

***Beneficial owner***

Beneficial owner is a natural person for the benefit of whom a transaction is being carried out or a natural person who

- i. has a direct or indirect interest or their total at least 25 % in the equity capital or in voting rights in a customer being a legal person - entrepreneur, including bearer shares, unless that legal person is an issuer of securities

admitted to trading on a regulated market who is subject to disclosure requirements under a special regulation;<sup>9)</sup>

- ii. is entitled to appoint, otherwise constitute or recall a statutory body, a majority of members of a statutory body, a majority of Supervisory Board members or other executive body, supervisory authority or auditing authority of a customer being a legal person -entrepreneur;
- iii. in a manner other than those set forth in subsections 1 and 2 controls a customer that is a legal person -entrepreneur;
- iv. is a founder, a statutory body, a member of a statutory body or of other executive body, supervisory authority or auditing authority of a customer being an corporation or is entitled to appoint, otherwise constitute or recall those authorities;
- v. is a beneficiary of at least 25% of funds distributed by an corporation, provided the future beneficiaries of those funds are designated or
- vi. ranks among those persons for whose benefit an corporation is established or operates, unless the future beneficiaries of funds of the corporation are designated,

### ***Identification threshold amount***

(2) Obligated entity shall be obliged to perform customer due diligence

- a) at the moment of establishment of a business relationship,
- b) when carrying out an occasional transaction outside a business relationship worth at least EUR 15,000 regardless of whether the transaction is carried out in a single operation or in several related operations which are or may be linked,
- c) if there is a suspicion that the customer is preparing or carrying out an unusual transaction regardless of the amount of the transaction,
- d) when there are doubts about the veracity or completeness of customer identification data previously obtained, or
- e) where concerning withdrawal of a cancelled final balance of bearer deposit.

(3) Obligated entity shall be obliged to perform the identification of a customer and verification of his identification also in case of carrying out a transaction the amount of at least EUR 2,000, unless concerning any of the case under subsection 2.

---

<sup>9)</sup> Act No. 566/2001 Coll. as amended

***Identification at a distance (non face to face)***

*Section 7*

Identification for the purposes of this Act, shall be understood upon performance by third parties under Section 13, receiving information and supporting underlying documentation from a credit institution or a financial institution.

**d. *Outsourcing of identification to third parties***

*Section 13*

(1) Obligated entity may receive data and documentation under Sec. 10, subsection 1, letters a) to c) which are required to perform customer due diligence from a credit institution or a financial institution under Sec. 5, subsection 1, letter b, items 1 to 10 which operates in the territory of a Member State.

(2) A credit institution or a financial institution which has already performed customer due diligence shall without delay supply data within the range of Sec. 10, subsection 1, letters a) to c), including copies of the respective documentation to an obliged entity proceeding under subsection 1 and providing for the receipt of data.

(3) The application of the procedure under subsection 1 shall not release the obliged entity from liability for the performance of customer due diligence under this Act.

(4) Business relationships of obliged entities with persons acting for the obliged entities on the basis of a contractual relationship other than employment shall not be regarded as performance by third parties.

**e. *Means of identification/verification***

*Section 8*

Verification of identification for the purposes of this Act, shall be understood:

- a) in the case of a natural person, verifying the data under Section 7, letter a) in his identification document, if contained therein, and verifying the appearance of that person by comparing it to his appearance on the identification document in his presence; in the case of a natural person being an entrepreneur, this shall also include verification of the data under Section 7, letter a) on the basis of documents, data or information

obtained from the official register or other official record in which the entrepreneur is entered or from other reliable and independent source;

- b) in the case of a legal person, verifying the data under Section 7, letter b) on the basis of documents, data or information obtained from the official register or other official record in which the legal person is entered or from other reliable and independent source, and verifying the identity of a natural person who is authorized to act on behalf of the legal person to extent of data under Section 7, letter a), in his physical, and verifying his power to act on behalf of the legal person;
- c) in the case of a person represented by virtue of a power of attorney, verifying his data to extent of data under Section 7, letter c) on the basis of documents, data or information obtained from the submitted power of attorney containing an authenticated signature, from the official register or other official record or from other reliable and independent source, and verifying the identification of a natural person who is authorized to act on the basis of the power of attorney to extent under Section 7, letter a), in his identification document in his physical;
- d) in the case of a minor person, who possesses no identification document, it verifying type and number of the identification document and appearance of the minor's legal guardian by comparing it to his appearance on the identification document;
- e) verifying identification number or code allocated to the customer for carrying out transactions by the obliged entity's technical device under a special regulation<sup>10)</sup>, provided the customer has already been identified under Sec. 7, letters a) to d);
- f) customer identifying himself by an electronic signature, provided the customer has already been identified under Sec. 7, letters a) to d); or
- g) verification of identification in different manner, if allowed so by a special regulation.

**f. Source of information (e.g.: public register for the identification of beneficial owner)**

see "e. Means of identification/verification".

[PRODUCTS AND TRANSACTIONS CHARACTERISED BY A HIGH/LOW RISK OF MONEY LAUNDERING]

*Section 4*

(1) Unusual transaction shall mean a legal or other act which indicates that its execution may enable legalization or terrorist financing.

(2) Unusual transaction shall above all mean a transaction:

- a) which, having regard to its complexity, unusually high amount of funds or its other nature, goes apparently beyond the common framework or nature of a certain type of transaction or a transaction of a certain customer;
- b) which, having regard to its complexity, unusually high amount of funds or its other nature, has no apparent economic purpose or lawful purpose;
- c) where the customer refuses to identify himself or to provide the information necessary for the obliged entity to perform customer due diligence referred to in Sections 10 to 12;
- d) where the customer refuses to provide details of the upcoming transaction, or tries to provide as little information as possible, or provides such information that it is possible to verify by the obliged entity only with great difficulty or vast expenses;
- e) where the customer demands its execution based on a project which raises doubts;
- f) where use is made of money of low nominal value in a considerably high amount;
- g) with a customer in whose case it can be presumed that given his occupation, position or other characteristics, he is not, or cannot be, the owner of the required funds;
- h) where the amount of funds available to the customer is apparently disproportionate to the nature or scope of his business activities or his declared financial position;
- i) where there is a reasonable assumption that the customer or beneficial owner is a person on whom international sanctions are imposed under a special regulation<sup>11)</sup>, or a person who is likely to be related to a person on whom international sanctions are imposed under a special regulation; or
- j) where there is a reasonable assumption that its subject is or is to be goods or a service that may relate to goods or a service on which international sanctions are imposed under a special regulation.

[EXISTING GUIDELINES TO THE BANKING INDUSTRY]

No guidelines yet

[GENERAL FEEDBACK (NEW MODUS OPERANDI, TRENDS, REAL CASES, etc)]

*Section 26*

The Financial Intelligence Unit shall:

---

<sup>11)</sup> Act No. 460/2002 Coll. on the Application of International Sanctions Assuring International Peace Settlement and Security as amended by Act No. 127/2005 Coll.

- a) disclose information on the forms and ways of legalization and terrorist financing and the methods of recognizing unusual transactions;
- b) inform the obliged entity on the effectiveness of unusual transaction report and on the procedures that follow receipt of unusual transaction report, unless there is a threat of hampering of the processing of the unusual transaction.

## [PURPOSES FOR WHICH THE FEEDBACK INFORMATION MAY BE USED]

No regulation in AML Act

## [PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK STAFF IN THE EVENT OF NOTIFICATION) OF THE INSTITUTIONS OR PERSONS COVERED BY THIS DIRECTIVE ]

### Section 26

(2) The Programme of the Obligated Entity must contain

- e) a procedure applied from the moment of detecting an unusual transaction to its immediate reporting to the Financial Intelligence Unit, including procedure and responsibility of employees evaluating the unusual transaction,
- i) the manner of ensuring the protection of employees who detects unusual transactions,
- j) the content and a schedule for special training of employees who may, in the course of performance of their occupation, come into contact with an unusual transaction,

## [CONSERVATION OF RECORDS AND DOCUMENTS]

### Section 19

(1) For customer due diligence purposes, an obliged entity shall be authorized, even without the consent of and notification to the persons concerned, to detect, obtain, record, keep, use or otherwise process<sup>12)</sup> personal data and other data to the extent under Sec. 10, subsection 1 and Sec. 12, subsections 1 and 2; in doing so, the obliged entity is authorized to obtain personal data necessary to achieve the purpose of processing by copying, scanning or other recording of official documents on a data carriers and process birth registration numbers and other data and documents without the consent of the person concerned<sup>13)</sup>, to the extent under Sec. 10, subsection 1 and Sec. 12, subsections 1 and 2.

---

<sup>12)</sup> Section 4, subsection 5 and Section 7, subsection 3 of Act No. 428/2002 Coll.

<sup>13)</sup> Sec. 10, subsection 6 of Act No. 428/2002 Coll.

(2) The obliged entity shall be obliged to keep for a period of five years:

- following the termination of its business relationship with the customer, data and written documents obtained under Sec. 10 to 12,
- from the moment of the carrying out a transaction, all data and written documents about it.

(3) Obligated entity shall be obliged to keep data and written documents under subsection 2 even for a period longer than five years if the Financial Intelligence Unit requests so in writing; the Financial Intelligence Unit in a request shall specify a period and extent to which the data and written documents shall be kept.

(4) Even a person who ceases to act as an obliged entity shall have the obligations under subsections 2 and 3 until the expiry of the period during which an obliged entity shall be obliged to keep the data and written documents under subsections 2 and 3.

[STEPS TAKEN TO INCREASE AWARENESS OF THE PHENOMENON OF MONEY LAUNDERING (E.G.: TRAINING, INFORMATION...)]

## *Section 26*

(3) Obligated entity shall be obliged to provide for special training of employees aimed to make them acquainted with the Programme, at least once a calendar year and always before assignment of the employee to a job position requiring the fulfilment of tasks under this Act. The obliged entity shall be obliged to ensure that the Programme is permanently available to each employee performing the tasks under this Act.

### [ANTI-MONEY LAUNDERING /CTF LEGISLATION]

Law on the Prevention of Money Laundering and Terrorist Financing (Act) No. 60 of 6 July 2007 which transposes the third AML Directive and replaces former Law on the Prevention Of Money Laundering.

The act authorises the Minister of Finance to enact several rules, which are already in force:

- Rules on the Method of Forwarding Information to the Office for Money Laundering Prevention of the Republic of Slovenia (Office)
- Rules laying down conditions to be met by a person to act in the role of a third party
- Rules on Performing Internal Control, Authorised Person, Safekeeping and Protection of Data and Keeping of Records of Organizations, Lawyers, Law firms and Notaries
- Rules on the Method of Communicating the Information on Lawyers, Law Firms or Notaries to the Office for Money Laundering Prevention of the Republic of Slovenia
- Rules laying down conditions under which a person may be considered as a customer representing a low risk of money laundering or terrorist financing
- Rules laying down the list of equivalent third countries
- Rules laying down conditions under which there is no obligation to report cash transaction data for certain customers
- Rules laying down conditions to determine and verify customer's identity by using customer's qualified digital certificate

### [PENALTIES IN NATIONAL LAW FOR FAILURE TO RESPECT OF THE NATIONAL PROVISIONS TO THE DIRECTIVE]

**The act imposes several penalties and differs penalties between:**

**1) Most serious offences** (i.e.: failure to prepare a risk analysis or establish a risk assessment for individual groups or customers, business relationships, products or transactions; failure to carry out customer due diligence; establishing a business relationship with a customer without

prior application of the prescribed measures; effecting a transaction without prior application of the prescribed measures; failure to determine and verify the identity of a natural person or his/her statutory representative, sole proprietor or self-employed person, legal entity, statutory representative of a legal entity, authorised person, agent of other civil law entities or beneficial owner of the legal entity or similar foreign law entity, or failure to obtain the prescribed data, or failure to obtain them in the prescribed manner, or failure to obtain the certified written authorisation for representation, etc ...) **for legal entities** which are prescribed from EUR 12.000 to 120.000.

A fine from EUR 800 to EUR 4,000 shall be imposed on the responsible **person of a legal entity**, sole proprietor or self-employed person for the offences stated above.

A fine from EUR 4,000 to 40,000 shall be imposed on **a sole proprietor or self-employed person** for the offences stated above.

**2) Serious offences** (i.e.: failure to carry out customer due diligence within the prescribed scope; failure to define procedures for implementation of the prescribed measures in its internal regulations; failure to demand a written statement from the customer, statutory representative, failure to monitor business activities undertaken by a customer through the organisation with due diligence entrusting a third party to carry out customer due diligence without having verified whether that third party meets all the conditions stipulated by this Act, etc...) **for legal entities** which are prescribed from EUR 6,000 to 60,000.

A fine from EUR 400 to 2,000 shall be imposed on the **responsible person** of a legal entity, sole proprietor or self-employed person for the offences stated above.

A fine from EUR 2,000 to 20,000 shall be imposed on **a sole proprietor** or a self-employed person for the s stated above.

**3) Minor offences** (i.e.: failure to examine beforehand, when determining and verifying the identity of a customer, the nature of the register from which data on the customer shall be obtained; failure to inform the Office for Money Laundering Prevention of the Republic of Slovenia (Office) and take appropriate measures to eliminate the risk of money laundering or terrorist financing; failure to inform its branches and majority-owned subsidiaries with head offices in third countries of the internal procedures relating to the detection and prevention of money laundering and terrorist financing, etc..) **for legal entities**, which are prescribed from EUR 3.000 to 30.000.

A fine from EUR 200 to EUR 1,000 shall be imposed on the **responsible person** of a legal entity, sole proprietor or self-employed person for the offences stated above.

A fine from EUR 1,000 to 10,000 shall be imposed on a **sole proprietor** or **self-employed person** for the offences stated above.

Among persons, stated above, employees of organisations, auditing firms, independent auditors, legal entities and natural persons performing accounting or tax advisory services, lawyers, law firms and notaries and persons pursuing the activity of selling goods are also responsible for the some offences and could be penalized from EUR 200 (employees) to 120.000 (auditing firms, independent auditors, legal entities and natural persons performing accounting or tax advisory services).

## [CENTRAL AUTHORITY FOR REPORTING]

Central authority for reporting in the Republic of Slovenia is the Office for Money Laundering Prevention of the Republic of Slovenia (Office).

## [PERSONS RESPONSIBLE FOR REPORTING]

Every person under obligation (see next title) has to nominate an authorised person and one or more deputies. The exceptions are organisations of fewer than four employees who are not to be required to appoint an authorised person.

## [BUSINESS COVERED BY THE LEGISLATION (WHICH SPECIFIC PERSONS: NOTARIES, LAWYERS...)]

Persons (further on: organisations) who are under obligations of Act, are:

1. banks, branches of banks from third countries and Member State banks which establish branches in the Republic of Slovenia or which are authorised to directly perform banking services in the Republic of Slovenia;
2. savings banks;
3. companies providing certain payment transaction services, including money transmission;
4. post;
5. management companies of investment funds, branches of management companies of investment funds from third countries, management companies of investment funds from Member States which establish branches in the Republic of Slovenia or are authorised to provide services of investment fund management in the Republic of Slovenia, and other persons who may provide particular services or activities of managing investment funds pursuant to the Act governing investment fund management;
6. founders and managers of mutual pension funds and pension companies;
7. brokerage companies, branches of brokerage companies from third countries, brokerage companies from Member States which establish branches in the Republic of Slovenia or are authorised to provide services relating to securities directly in the

Republic of Slovenia, and other persons who may provide particular services relating to securities pursuant to the Act governing the securities market or the Act governing the financial instruments market;

8. insurance companies authorised to pursue life insurance business and insurance companies from Member States which establish branches in the Republic of Slovenia or which are authorised to pursue life insurance business directly in the Republic of Slovenia;
9. electronic money undertakings, branches of electronic money undertakings from third countries, and electronic money undertakings from Member States which establish branches in the Republic of Slovenia or which are authorised to provide electronic money services directly in the Republic of Slovenia;
10. currency exchange offices;
11. auditing firms and independent auditors;
12. concessionaires organising special gaming in casinos or gaming halls;
13. organisers regularly offering sport wagers;
14. organisers and concessionaires offering games of chance via the Internet or other telecommunications means;
15. pawnbroker shops;
16. legal entities and natural persons conducting business relating to:
  - a) granting credits or loans, also including consumer credits, mortgage credits, factoring and financing of commercial transactions, including forfeiting;
  - b) financial leasing;
  - c) issuing and management of payment instruments (such as credit cards and travellers' cheques);
  - d) issuing of guarantees and other commitments;
  - e) portfolio management services to third parties and related advice;
  - f) safe custody services;
  - g) mediation in the conclusion of loan and credit transactions;
  - h) insurance agency services for the purpose of concluding life insurance contracts;
  - i) insurance intermediaries in concluding life insurance contracts;
  - j) accounting services;
  - k) tax advisory services;
  - l) trust and company services;

- m) trade in precious metals and precious stones and products made from these materials;
- n) trade in works of art;
- o) organisation and execution of auctions;
- (p) real property transactions

Pursuant to the provisions of Chapter III by present Act, the measures for detecting and preventing money laundering and terrorist financing stipulated must be applied by lawyers, law firms and notaries as well.

## [PREDICATE OFFENCES COVERED]

Predicate offences cover any conduct for the purpose of disguising the origin of money or other property obtained by an offence and shall include:

1. Conversion or any transfer of money or other property derived from criminal activity;
2. Concealment or disguise of the true nature, origin, location, movement, disposition, ownership or rights with respect to money or other property derived from criminal activity.
3. Terrorist financing

## [IDENTIFICATION]

### **a) Definition (e.g.: PEPs, beneficial owner, thresholds...)**

#### **PEPs**

The politically exposed person shall mean any natural person who is or has been entrusted with prominent public function in the previous year and resides in another Member State or in a third country, or a person who is or has been entrusted with prominent public function in another Member State or in a third country in the previous year, including immediate family members and close associates.

(3) Natural persons who are or have been entrusted with prominent public function shall be the following:

1. heads of state, prime ministers, ministers and their deputies or assistants;
2. elected representatives in legislative bodies;

3. members of supreme and constitutional courts and other high-level judicial authorities against whose decisions there is no ordinary or extraordinary legal remedy, save in exceptional cases;
4. members of courts of audit and boards of governors of central banks;
5. ambassadors, *chargés d'affaire* and high-ranking officers of armed forces;
6. members of the management or supervisory bodies of undertakings in majority state ownership.

(4) Immediate family members of the person shall be the following: spouse, common law partner, parents, brothers and sisters and children and their spouses or common law partners.

(5) The close associate shall mean any natural person who has a joint profit from property or business relationship or has any other close business links.

**b) Identification threshold amount**

Identification must be verified, when the sum involved is 15.000 or more, or whenever money laundering is suspected regardless of the amount.

**c) Identification at a distance (non face to face)**

The organisation should verify in advance whether the **third party** entrusted to carry out customer due diligence meets all the conditions stipulated by the Act.

Customer due diligence performed for the organisation by a third party may not be accepted as appropriate if, within this procedure, the third party determined and verified the identity of a customer in his/her absence.

The organisation which relies on a third party in respect of customer due diligence shall remain responsible for the proper customer due diligence procedure under this Act.

**The third party could be:** banks, branches of banks from third countries and Member State (EU members) banks which establish branches in the Republic of Slovenia or which are authorised to directly perform banking services in the Republic of Slovenia; savings banks; post; management companies of investment funds, branches of management companies of investment funds from third countries, management companies of investment funds from EU Member States (Member State) which establish branches in the Republic of Slovenia or are authorised to provide services of investment fund management in the Republic of Slovenia, and other persons who may provide particular services or activities of managing investment funds pursuant to the Act governing investment fund management; founders and managers of mutual pension funds and pension companies; brokerage companies, branches of brokerage companies from third countries,

brokerage companies from Member States which establish branches in the Republic of Slovenia or are authorised to provide services relating to securities directly in the Republic of Slovenia, and other persons who may provide particular services relating to securities pursuant to the Act governing the securities market or the Act governing the financial instruments market; insurance companies authorised to pursue life insurance business and insurance companies from Member States which establish branches in the Republic of Slovenia or which are authorised to pursue life insurance business directly in the Republic of Slovenia; a bank of a Member State or a branch of a Slovenian bank in a Member State; an investment fund management company from a Member State or a branch of a Slovenian investment fund management company in a Member State; founders or managers of mutual pension funds from a Member State or a pension company from a Member State; a brokerage company from a Member State or a branch of a Slovenian brokerage company in a Member State; an insurance company from a Member State or a branch of a Slovenian insurance company in a Member State; a branch or subsidiary of a bank from a Member State in a third country, a branch or subsidiary of a management company from a Member State in a third country, a branch or subsidiary of a brokerage company from a Member State in a third country, or a branch or subsidiary of an insurance company from a Member State in a third country; a notary situated in a Member State or in an equivalent third country (third country is a country, who comply FATF - EU anti money laundry standards).

**d) Means of identification**

Identification must be obtained when establishing a business relationship with a customer; when carrying out a transaction amounting to EUR 15,000 or more, whether the transaction is carried out in a single operation or in several operations which are evidently linked and whenever there is a suspicion of money laundering or terrorist financing in respect of a transaction or customer, regardless of the transaction amount.

Identification means:

- establishing the customer's identity and verifying the customer's identity on the basis of authentic, independent and objective sources on the base of customers official personal identification document (individuals and statutory representative of the company); for companies must be obtain the original or certified documentation from the court register or other public register.
- determining the beneficial owner of the customer;
- obtaining data on the purpose and intended nature of the business relationship or transaction, as well as other data pursuant to Act.

**e) beneficial owner**

Pursuant to the Act, the beneficial owner of a corporate entity is:

1. any natural person who owns through direct or indirect ownership at least 25% of the business share, stocks or voting or other rights, on the basis of which he/she participates in the management or in the capital of the legal entity with at least 25% share or has the controlling position in the management of the legal entity's funds;
2. any natural person who indirectly provides or is providing funds to a legal entity and is on such grounds given the possibility of exercising control, guiding or otherwise substantially influencing the decisions of the management or other administrative body of the legal entity concerning financing and business operations.

For the purposes of the Act, the beneficial owner of other legal entities, such as foundations and similar foreign law entities which accept, administer or distribute funds for particular purposes shall mean:

1. any natural person who is the beneficiary of more than 25% of the proceeds of property under management, where the future beneficiaries have already been determined or can be determined;
2. a person or a group of persons in whose main interest the legal entity or similar foreign law entity is set up and operates, where the individuals that benefit from the legal entity or similar foreign law entity have yet to be determined;
3. any natural person exercising direct or indirect control over 25% or more of the property of a legal entity or similar foreign law entity.

## [PRODUCTS AND TRANSACTIONS CHARACTERISED BY A HIGH/LOW RISK OF MONEY LAUNDERING]

For identifying transactions with high risk, banks must compile a list of indicators for the identification of customers and transactions in respect of which reasonable grounds to suspect money laundering or terrorist financing exist.

However, banks must classify customers among: enhanced due diligence, regular due diligence and simplified due diligence. Estimation whether transactions are high or low risk of money laundering depends also of this classification of the customer.

Otherwise, products or transactions, characterised by a low/high risk of money laundering are not listed in Act or in other rule/manual.

## [EXISTING GUIDELINES TO THE BANKING INDUSTRY]

Recommendations for applying Act were issued by our The Bank Association of Slovenia. Besides this, The Bank of Slovenia (central bank) is preparing rules as well.

## [GENERAL FEEDBACK (NEW MODUS OPERANDI, TRENDS, REAL CASES, etc)]

In accordance with Act, the Office must notify in writing the person who report suspicious transaction of the completion of collecting and analysing data, information and documentation in connection with a certain person or transactions in respect of which there are grounds to suspect money laundering or terrorist financing, or established facts that indicate or may indicate money laundering or terrorist financing, unless the Office judges that such action may jeopardise further proceedings.

## [PURPOSES FOR WHICH THE FEEDBACK INFORMATION MAY BE USED]

The feedback information is used as support in the activities of reporting company/person.

## [PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK STAFF IN THE EVENT OF NOTIFICATION) OF THE INSTITUTIONS OR PERSONS COVERED BY THIS DIRECTIVE ]

Protection of employees of the institutions and persons covered by Directive is prescribed in Act:

(1) The organisation, lawyer, law firm, notary and staff shall not be held liable for the damage caused to customers or to third persons if, in compliance with the provisions of this Act or the ensuing regulations, they:

1. submit to the Office data, information and documentation on their customers;
2. obtain and process data, information and documentation on their customers;
3. implement an order on temporary suspension of the transaction or the instruction issued in connection with the said order;
4. implement a request by the Office for the ongoing monitoring of the customer's financial transactions.

(2) The staff of organisations, law firms and notaries shall not be held criminally or disciplinarily liable for the breach of obligation to protect classified data, business and bank secrecy and professional secrecy due to:

1. their submission of data, information and documentation to the Office in accordance with the provisions of this Act or the ensuing regulations;
2. their processing of data, information and documentation obtained in accordance with this Act, for the purpose of verifying customers and transactions in respect of which there are grounds to suspect money laundering or terrorist financing.

## [CONSERVATION OF RECORDS AND DOCUMENTS]

Records and documents must be retained for a period of 10 years after the termination of a business relationship or the completion of a transaction.

## [STEPS TAKEN TO INCREASE AWARENESS OF THE PHENOMENON OF MONEY LAUNDERING (E.G.: TRAINING, INFORMATION...)]

The Act requires that organisation must provide regular professional training and education for all employees carrying out tasks for the prevention and detection of money laundering and terrorist financing.

To meet the Act requirements, seminars are also organized by our association together with state supervisors.

### [ANTI-MONEY LAUNDERING /CTF LEGISLATION]

- Law 12/2003, of 21 May, on the prevention of terrorism financing and freezing of funds.
- Law 19/1993, of 28 December on specific measures for the prevention of money laundering (revised by Law 19/2003, of 4 July, and Law 39/2006, of 29 November).
- Royal Decree 925/1995, of 9 June, implementing regulations of Law 19/1993 (revised by Royal Decree 54/2005, of 21 January)
- Ministerial Order EHA/2619/2006, of 28 July, setting specific obligations on the prevention of money laundering for institutions and persons carrying activities of currency exchange and cross border transfers.
- Ministerial Order EHA/1439/2006, of 3 May, on the obligation to declare movements of cash and other means of payment.
- Ministerial Order EHA/2444/2007, of 31 July, on the external annual report to be issued on the compliance with the procedures, internal control and communication obligations required for the prevention of money laundering.
- Resolution of the Ministry of Finance, of 10 September 2008, containing the list of equivalent countries.

*Directive 2005/60/CE, of 26 October 2005, has not been transposed yet into Spanish legislation. Therefore, all the information provided below refers to current legislation.*

### [PENALTIES IN NATIONAL LAW FOR FAILURE TO RESPECT OF THE NATIONAL PROVISIONS TO THE DIRECTIVE]

Law 19/2003 defines precisely which sanctions can be imposed for breach of obligations contained in the Law. Offences are classified as serious and very serious. Examples of very serious offences are informing customers that reporting has been transmitted to SEPBLAC (Spanish FIU); non reporting transactions to the FIU, or resistance to provide any information requested by the FIU.

Penalties for serious breaches:

- For companies: a) private or public warning; b) a minimum fine of € 6,000 and a maximum of 1% of the company's own funds, or 100% of the amount of the transaction increased by 50% or €150,000.
- For management: a) private or public warning; b) fine for minimum amount of €3,000 and a maximum of €60,000; c) suspension from exercising his duties for up to one year.

Penalties for very serious breaches:

- For companies:
  - public warning;
  - a minimum fine of €90,000 and a maximum of 5% of own funds, or 200% of the transaction, or €1.5 million.
- For management:
  - a fine amounting between €60,000 and €600,000;
  - disqualification from exercising his duties in the same entity for a period of five years;
  - disqualification on management positions in any other entity within the scope of Law No. 19/1993 for ten years.

## [CENTRAL AUTHORITY FOR REPORTING]

The Executive Service of the Commission for the Prevention of Money Laundering and Monetary offences (known by its Spanish abbreviation SEPBLAC) is the central authority for reporting. The Commission is headed by the Secretary of State for Economy.

The functions of the SEPBLAC, who is the Spain's Financial Intelligence Unit, are as follows:

- Rendering assistance to the judicial bodies, the Public Prosecution Department, the criminal police and the competent administrative bodies.
- Reporting to these bodies and institutions on the conduct giving reasonable indications of a criminal offence or, as the case may be, an administrative infringement.
- Receiving the communications and information that subject persons are obliged to send concerning any event and transaction with regard to which there is reason to believe or certainty that it is related to money laundering. These reports may be submitted at the initiative of the subject persons or they may be required by the Executive Service.
- Analysing the information received and taking the further action called for in each case.

- Carrying out the instructions and following the guidelines given by the Commission, and submitting to it the reports that it requests.
- Monitoring the suitability of the internal control and communication procedures and bodies established by the parties subject to anti-money laundering law and proposing the necessary corrective measures.

## [PERSONS RESPONSIBLE FOR REPORTING]

Each credit institution can organise itself internally in the way it feels is the most appropriate in order to prevent money laundering, collect information from branches, analyse evidence of offences or suspect operations, and to communicate it to the competent authority. The procedures adopted are supervised by the SEPBLAC (Spanish FIU) and must be evaluated annually by an external expert.

In any event, all the credit institution must establish the necessary internal control bodies and designate a permanent representative as a contact point for dealings with the Executive Service of the Commission for the Prevention of Money Laundering (SEPBLAC) and any other administrative or judicial authority. The permanent representative has to comply with the requirements established by legal regulations and has to be appointed by the board of directors with the approval of the SEPBLAC.

## [BUSINESS COVERED BY THE LEGISLATION (WHICH SPECIFIC PERSONS: NOTARIES, LAWYERS...)]

The law cover the following legal or natural “subject persons”:

a) all forms of financial institutions:

- credit institutions;
- insurance companies;
- investment firms;
- undertakings for collective investment;
- portfolio management companies;
- stockbrokers;
- companies issuing credit cards;
- companies and natural persons carrying on foreign exchange business or cross border transfers.

b) non-financial enterprises, i.e. expressly including:

- real estate companies and agents;
- notaries, lawyers and attorneys ;
- auditors, accountants and tax advisors;
- casinos;
- jewellers;
- antique shops
- institutions involved in numismatics and philately.

Persons included in a) or b) groups are subject to different obligations.

## [PREDICATE OFFENCES COVERED]

Law 19/1993 on measures to prevent money laundering regulates obligations of banks and other financial institutions in order to prevent money laundering and to avoid any other crime punishable by a prison term of more than three years, as well as penalties for breaches of such obligations, irrespective of the responsibilities or penalties that might arise from the Criminal Code.

## [IDENTIFICATION]

### **a. Definition (e.g.: PEPs, beneficial owner, thresholds...)**

Law 19/1993 does not include definitions of PEPs, beneficial owner or others, which could be adopted when Directive 2005/60/EC is transposed.

### **b. Identification threshold amount**

As a general rule, banks are required to identify any person with whom permanent business relationship is established by opening an account or any other transactions, regardless of the amount of the transaction.

In the case of an occasional customer, credit institutions must identify the customer if the amount of the transaction exceeds €3,000. However, in cross-border transfers or currency exchange operations the client must be always identified when the transaction is not recorded in an account.

**c. Identification at a distance (non face to face)**

The legislation in force allows credit institutions to start business relationship or conduct operations at a distance (by telephone or electronic banking), without the physical presence of the customer for identification, if the identity of the customer is credited by certified electronic signature or the first entry of the account comes from another account opened by the same customer in Spain or in a country with equivalent regulation. In any case, within a month a copy of an official identification document must be given.

**d. Outsourcing of identification to third parties**

No regulation in force.

**e. Means of identification**

Under the Royal Decree 925/2005, the means of customer identification are the following:

**Natural persons**

- Spanish citizen: national identity card;
- Foreign resident: residence permit.
- Non-resident foreigner: passport or national identity card.

**Legal persons**

- Spanish legal persons: Tax Registration Number; official articles of association and statutes;
- Foreign legal persons; documents proving that they have been validly constituted, in accordance with the legislation applicable to their status;
- Non-commercial communities, associations and other bodies: documents proving their legal constitution.

**f. Source of information (e.g.: public register for the identification of beneficial owner)**

There is no public register to allow the identification of the beneficiary owner. The Business Register offers the possibility of obtaining certain data on legal persons.

## [PRODUCTS AND TRANSACTIONS CHARACTERISED BY A HIGH/LOW RISK OF MONEY LAUNDERING]

The regulations in force identifies areas of activity that require special identification measures, such as private banking, correspondent banking, remote banking, currency exchange and cross border transfers.

## [EXISTING GUIDELINES TO THE BANKING INDUSTRY]

There are no formal guidelines other than the existing regulations in force that are very detailed.

## [GENERAL FEEDBACK (NEW MODUS OPERANDI, TRENDS, REAL CASES, etc)]

No formal or regular feedback on reporting transactions, while the SEPBLAC (Spanish FIU) periodically organizes meetings in which information is provided on the new modus operandi, trends, real cases, and so on.

## [PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK STAFF IN THE EVENT OF NOTIFICATION) OF THE INSTITUTIONS OR PERSONS COVERED BY THIS DIRECTIVE ]

Law 19/1993 exempts from any responsibility to bank managers' and bank employees' for reporting suspicious transactions or providing to the SEPBLAC (Spanish FIU) any requested information. An additional protection to employees is provided by the legislation since the permanent representative that has to be appointed by each credit institution is the only person to maintain relationship with the SEPBLAC or any other authority

## [CONSERVATION OF RECORDS AND DOCUMENTS]

### **a) Duration**

Documents serving as evidence of operations carried out (and where appropriate computer records) and copy of those relating to identity must be retained for a period of at least 6 years.

### **b) Means of conservation.**

There are no specific provisions in this matter.

[STEPS TAKEN TO INCREASE AWARENESS OF THE PHENOMENON OF MONEY LAUNDERING (E.G.: TRAINING, INFORMATION...)]

In general, the legislation requires institutions and persons covered by the Law to take appropriate measures for employees, and especially for those who are in a better position to detect money laundering transactions, to be aware of obligations under the Law on prevention of money laundering.

Credit institutions develop regularly training programmes, aimed in particular at employees in direct contact with customers, internal seminars, etc.

## SWEDEN

The Swedish Bankers' Association

### [ANTI-MONEY LAUNDERING /CTF LEGISLATION]

- The Money Laundering Act from 1993. Latest amendments came into force on the 1<sup>st</sup> January 2005.
- The Terrorism Acts that came into force in 2002 and 2003

Currently, the Swedish Government is incorporating the Third Money Laundering Directive (2005/60/EC) into Swedish law. The law is expected to come into force on the 15<sup>th</sup> March 2009.

### [PENALTIES IN NATIONAL LAW FOR FAILURE TO RESPECT OF THE NATIONAL PROVISIONS TO THE DIRECTIVE]

The management of the banks which fails to fulfil their obligation to report suspected money laundering transactions or transaction connected to financing of terrorism can be liable to a fine.

### [CENTRAL AUTHORITY FOR REPORTING]

The Financial Intelligence Police (FIPO), a part of the National Police Board.

### [PERSONS RESPONSIBLE FOR REPORTING]

The board of directors must establish an overall policy regarding measures against money laundering and financing of particularly serious crimes. Then, there are designated persons within the Security and Legal Departments of the banks who have the daily responsibility for reporting.

### [BUSINESS COVERED BY THE LEGISLATION (WHICH SPECIFIC PERSONS: NOTARIES, LAWYERS...)]

- Banks, credit market companies and mortgage companies and other credit institutions.
- Financial Institutions, e.g. Money services business; bureaux de change and money transmitters.

- Fund management companies
- Securities companies
- Life insurance companies
- Companies administrating funds
- Insurance brokers
- Electronic Money Institutions
- Auditors (after 15 March 2009 the Act will also include accountants)
- Tax consultants
- Estate agents
- Lawyers and other independent legal professional
- Casinos and dealers in high-value goods
- Deposit companies

The new Act will also include corporate services providers and company formation agents.

[PREDICATE OFFENCES COVERED]

[IDENTIFICATION]

**a. Definition (e.g.: PEPs, beneficial owner, thresholds...)**

The legislation does not specify PEPs or beneficial owners. The new law will contain a general definition of PEPs and beneficial owner. The Financial Supervisory Authority will most likely issue regulation with a definition of PEP and beneficial owner.

**b. Identification threshold amount**

The identification must be verified at the start of a business relationship or when one or more transactions are made at a total amount of EUR 15 000 without any business relationship starting. Identification is also needed whenever money laundering is suspected.

**c. Identification at a distance (non-face to face)**

The identification of a natural and legal persons must be carried out by means of documents or information which the undertaking obtains in writing or in another manner from the customer, from a third party or from internal or external registers. External register may be credit information registers and registers at governmental authorities such as population registers or business registers.

Verification of the identity at a distance must be carried out through a combination of controls of:

- Signature verified against certified copy of the identity document
- Information regarding personal identification number, company registration number, company signatory and board of directors, address, employer, credit card number, and numbers on identity documents compared against information in internal or external registers.
- Electronic methods for identification.
- Telephone call-backs or exchanges of faxes.

**d. Outsourcing of identification to third parties**

Natural and legal persons shall be identified in the same manner as set forth for the institutions and companies under the Money Laundering Act.

**e. Means of identification**

**Natural persons**

Verification of the identity must be carried out on the basis of valid certified identity cards, driving licence or passports issued following the expiry of 1997. Non-residents can verify their identity by a valid passport or other identity documents issued by governmental authority other authorised issuer.

**Legal persons**

Verification of a legal person and information regarding legal representatives shall be made on the basis of a registration certificate or other authorising documents.

**f. Source of information (e.g.: public register for the identification of beneficial owner)**

Please see the information set out above. Sweden does not have any official register for identification of beneficial owners.

[PRODUCTS AND TRANSACTIONS CHARACTERISED BY A HIGH/LOW RISK OF MONEY LAUNDERING]

The legislation in force today regulates lower risk regarding verification of identity if the company is a bank within the EU.

The new legislation will contain rules of both high and low risk of products and transactions.

[EXISTING GUIDELINES TO THE BANKING INDUSTRY]

The Financial Supervisory Authority has issued General Guidelines governing measures against Money laundering and Financing of particular serious crimes. Updated guidelines is expected to be published in July 2009.

[GENERAL FEEDBACK (NEW MODUS OPERANDI, TRENDS, REAL CASES, etc)]

The FIPO acknowledge receipt of every bank notification and present general feedback at regular meetings with the banking industry.

[PURPOSES FOR WHICH THE FEEDBACK INFORMATION MAY BE USED]

The information may only be used for criminal investigations and for prosecutions.

[PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK STAFF IN THE EVENT OF NOTIFICATION) OF THE INSTITUTIONS OR PERSONS COVERED BY THIS DIRECTIVE ]

Disclosure made in good faith by an employee is not treated as a breach of any restriction on the disclosure of information.

[CONSERVATION OF RECORDS AND DOCUMENTS]

Information regarding documentation in conjunction with verification of identity shall be preserved for not less than five years following termination of the business relationship. Information and documentation according to the Act on Bookkeeping shall be preserved for a

period not shorter than ten years after the termination of the financial year following the operation.

[STEPS TAKEN TO INCREASE AWARENESS OF THE PHENOMENON OF MONEY LAUNDERING (E.G.: TRAINING, INFORMATION...)]

The Association has produced an e-learning education based on the third Money Laundering Directive. Further, the Association has, in co-operation with the Financial Supervisory Authority produced written information both for the banks and for customers so that they can be informed about the obligations imposed on banks in order to combat money laundering. Also, the Associations have, together with its members, written guidelines for the banking industry.

The Financial Supervisory Authority has provided general guidelines governing measures pursuant to the Money Laundering Act and the Financing of Particular Serious Crimes Act. The Authority also presents new information continuously on their website for the banking industry.

## SWITZERLAND

Swiss Bankers Association (SBA)

### [ANTI-MONEY LAUNDERING /CTF LEGISLATION]

- Article 305bis (Money Laundering) and Article 305ter (negligence in relation to financial transactions) of the Penal Code have been in force since 1 August 1990.
- Article 305ter paragraph 2 of the Penal Code (right of communication of financial institutions) came into force on 1 August 1994.
- Federal law concerning the fight against money laundering in the financial sector (Money Laundering Law; administrative), in force since 1 April 1998.
- Government ordinance on the Money Laundering Reporting Office (MROS), in force since 1 October 2001.
- Money Laundering Ordinance of the Swiss Financial Market Supervisory Authority (FINMA), in force since 1 July 2003; (“*risk based*”; replaced the former Directives of the FINMA relating to the prevention of and fight against money laundering of 1998; current version 1.07.2008).
- Swiss Banks’ Code of Conduct with regard to the exercise of due diligence, came into force on 1 July 1977 (“*risk based too*”; current version CDB 08; 1.07.2008).
- Ordinance of the Federal Casino Commission on the diligence duties of casinos in combating money laundering, in force since 1 April 2000.
- Ordinance of the Swiss Financial Market Supervisory Authority (FINMA) for Insurance Matters on the prevention of money laundering, in force since 1 September 1999.
- Ordinance of the Swiss Financial Market Supervisory Authority (FINMA) for the Combat of Money Laundering on diligence duties of financial intermediaries under its control, in force since 1 January 2004

### [PENALTIES IN NATIONAL LAW FOR FAILURE TO RESPECT OF THE NATIONAL PROVISIONS TO THE DIRECTIVE]

- Law and Ordinance: Unlimited fines, withdrawal of licenses, work prohibition for employees.
- Swiss Banks’Code of Conduct: A fine of up to CHF 10 million

## [CENTRAL AUTHORITY FOR REPORTING]

Since 1 April 1998, Article 9 of the Federal Law on money laundering makes it compulsory for financial intermediaries to give notification when they know or presume, on the basis of founded suspicion, that assets involved in a business relationship are related to an infraction as defined in Article 305bis the Penal Code (money laundering), or are the proceeds of serious crime or are controlled by a criminal organisation. Violation of that duty to report is punishable by fine, licensed financial institutions shall be sanctioned by the regulator, i.e. the Financial Markets Supervisory Authority

This notification must be made to the Money Laundering Reporting Office (MROS), an administrative body (Financial intelligence unit) which reports to the Federal Office for Police. However and in accordance with Article 305ter paragraph 2 of the Penal Code, financial intermediaries still have the possibility to exercise their right of communication to the Swiss criminal authorities and/or the MROS when they believe that assets may originate from serious crime.

## [PERSONS RESPONSIBLE FOR REPORTING]

The Money Laundering law provides for all financial intermediaries an obligation to take organisational measures against ML, in particular education of staff and establishment of control measures. The relevant ordinances for the different institutions in the financial sector (banks, insurance companies, asset managers etc.) provide that financial intermediaries shall establish specialized AML units within the firm. They also provide detailed tasks for such units such as issuing directives, setting parameters for transaction monitoring systems etc. Experience shows that this will involve one or more persons, even possibly a specialized compliance department specialising in all matters pertaining to the fight against money laundering. A small bank may outsource this task (for example to its parent company or to an authorised auditing firm). However, the responsibility for proper AML management remains within the bank, and the bank will be sanctioned if it defaults.

## [BUSINESS COVERED BY THE LEGISLATION (WHICH SPECIFIC PERSONS: NOTARIES, LAWYERS...)]

### **Penal Code**

Article 305bis of the Penal Code covers everybody. Article 305ter of the Penal Code covers all financial transactions executed by professionals, without highlighting any specific professions.

### **Money Laundering Law**

The Money Laundering law covers anti-money laundering measures and the vigilance to be exercised with regard to financial transactions. Article 2 of that law defines the scope of application of the law. The law applies to financial intermediaries.

The following are considered as financial intermediaries (Article 2 § 2; financial intermediaries with prudential supervision):

- banks as defined in the law on banks;

- fund managers as defined in the Federal law of 18 March 1994 on undertakings for collective investment in transferable securities if they manage unit accounts or if they offer or distribute units in undertakings for collective investment in transferable securities;
- insurance companies as defined in the law on the supervision of insurance if their business includes life insurance, or if they offer or distribute units in undertakings for collective investment in transferable securities;
- stockbrokers as defined in the law of 24 March 1995 on stock exchanges.
- casinos as defined in the law of 18 December 1998 on casinos.

The following are also considered as financial intermediaries (Article 2 § 3): Persons, who, professionally, accept, hold as custodians or help to invest or invest assets belonging to third parties, in particular persons who:

- carry out credit transactions (in particular consumer or mortgage credits, factoring, trade finance or financial leasing);
- provide payment services, notably as regards electronic transfers for the account of third parties, or who issue or administer payment means such as credit cards and travellers cheques;
- trade in, for their own account or for the account of third parties, bank notes, money market instruments, currencies, precious metals, commodities or securities (physical instruments and rights) and their derivatives;
- offer or distribute units in undertakings for collective investment in transferable securities, as distributors of foreign or Swiss undertakings for collective investment in transferable securities as defined in the Federal law of 18 March 1994 on undertakings for collective investment in transferable securities or as representatives of a foreign undertaking for collective investment in transferable securities, provided that they are not subject to a supervisory body set up by a special law;
- carry out asset management business (includes attorneys and notaries public active in that kind of business);
- make investments as investment advisers (includes attorneys and notaries public active in that kind of business);
- act as custodians for or manage securities (includes attorneys and notaries public active in that kind of business).

The following are not covered by this law (Article 2 § 4):

- the Swiss National Bank (monetary authority);
- tax exempt occupational pension plans;
- persons providing services exclusively to tax exempt occupational pension plans;
- the financial intermediaries covered under paragraph 3 as providing services exclusively to the financial intermediaries listed in paragraph 2 or to foreign financial intermediaries subject to similar supervision.

## [PREDICATE OFFENCES COVERED]

The legislation covers all assets originating from serious crime (offences punished by penitentiary) or controlled by criminal organisations. Swiss legislation therefore does not provide a list of predicate offences, but implements the “threshold approach”.

## [IDENTIFICATION]

### **a. Definition (e.g.: PEPs, beneficial owner, thresholds...)**

Swiss law provides rules on identification of customers (individuals, legal entities or partnerships), identification of beneficial owners, and specific rules on client relationships to politically exposed persons. Politically exposed persons are defined in the FINMA ordinance 1 as persons performing important public functions in foreign states such as heads of state, politicians, high ranked public officials in administration, justice, army or in political parties, but also persons running states enterprises of national importance. Moreover also companies and persons close to the persons as mentioned before, be it for familiar, personal or business reasons, qualify as politically exposed persons.

### **b. Identification threshold amount**

When a business relationship is being established, financial intermediaries must verify the identity of the contracting party and - in case of doubt - must identify the beneficial owner, whatever the amount involved. The Money Laundering law sets no express limit above which cash transactions require an identification procedure. It is up to self-regulatory bodies implementing this law to fix such limits. For banks, the Due-Diligence Convention CDB 08 fixes this threshold at CHF 25'000.

### **c. Identification at a distance (non face to face)**

Where a business relationship is established by correspondence or via the internet, the bank must verify the identity of the contracting partner by obtaining an authenticated copy of an identification document as defined in point 9 above and checking the contracting partner's address either by postal delivery or by another equivalent method.

### **d. Outsourcing of identification to third parties**

The bank may, by written agreement only, appoint an individual or a company to verify the identity of a contracting partner, provided that

- a) it has instructed such mandatory as to its tasks and
- b) it is able to monitor the proper execution of the verification of identity.

The mandatory must forward all identification files to the bank and certify that any copies forwarded are identical to the corresponding originals. The appointment of a third party by the mandatory is prohibited. In any case, responsibility for correct CDD remains with the bank. The bank is exclusively liable towards the regulator and is also exposed to sanctions under the Code of Conduct.

**e. Means of identification**

The identification procedure includes checking the identity of the contracting party (which is a formal procedure based on official identity papers which must contain a photograph of the person) and the identification of the beneficial owner in case of doubt (which usually is based on a declaration by the contracting party, but can also consist in a formal identification by means of copies of the relevant documents). In the case of legal entities and partnership, the identity of the individuals establishing the business relationship must also be verified.

- **Verifying the contracting party's identity**

Natural persons: an official document with photograph;

Legal persons: extract from the Commercial Register or other official document (documents used for identification are photocopied; copies are to be filed by the financial intermediary.)

- **Identification of the beneficial owner**

The contracting party has to disclose the beneficial owner on Form A (full name, birthday, nationality, address and country of domicile) or Form T (for organised associations of individuals, assets or patrimony without specific beneficial owners);

- in case of doubt whether the contracting party is himself the beneficial owner of the funds or in the event of unusual circumstances;
- in the event of a power of attorney given to an unrelated third party;
- in the event of a business relationship established by correspondence with a natural person;
- in the case of a shell company/personal investment company/trust;

- **Attorneys and notaries:**

If their financial business is clearly connected to well defined legal mandates, they have to indicate to the bank the legal character of their mandate on a noname base (Form R); if their financial business is not clearly connected to well defined legal business, they have to indicate the beneficial owner on Form A.

Exception: between financial intermediaries (for example subject to banking supervision).

A declaration on Form A, R or T is a legal document. False declarations are punishable as a crime.

**f. Source of information (e.g.: public register for the identification of beneficial owner)**

- Federal Authorities of the Swiss Confederation; Legislation (<http://www.admin.ch>)
- Swiss Financial Market Supervisory Authority (FINMA; <http://www.finma.ch>)
- Swiss Bankers Association (<http://www.swissbanking.org>)

- Swiss Commercial Register (<http://www.zefix.admin.ch>)

## [PRODUCTS AND TRANSACTIONS CHARACTERISED BY A HIGH/LOW RISK OF MONEY LAUNDERING]

- if a client opens a relationship and deposits physically assets for more than CHF 100'000 at once or succeedingly.
- pass-through accounts if not based on the declared business profile of the client
- a transaction for which it is not clear why the customer wants to do it with a specific bank in a specific place (he could better do it elsewhere and with a more specialized partner)
- exchange of banknotes
- exchange of a considerable amount of cash without booking into a client account
- use of considerable amounts of cheques
- purchase or sale of precious metal by non-clients
- multiple cash transactions below the threshold (can be registered)
- repeated cash withdrawal without legitimate business purpose
- use of financial instruments that do not correspond to the normal investment activity of the client
- use of numbered accounts for commercial activities
- client tries to avoid personal contacts with bank employees
- many others

Relationships to politically exposed persons and relationships to correspondent banks must be qualified as enhanced risk relationships independently of the transactions.

## [EXISTING GUIDELINES TO THE BANKING INDUSTRY]

The Financial Markets Supervisory Authority joined to its AML ordinance lists of suspicious transactions that have to be investigated in by the bank.

## [GENERAL FEEDBACK (NEW MODUS OPERANDI, TRENDS, REAL CASES, etc)]

The relevant reports can be found on the pages of the Money Laundering Reporting Office MROS at [www.fedpol.admin.ch](http://www.fedpol.admin.ch)

## [PURPOSES FOR WHICH THE FEEDBACK INFORMATION MAY BE USED]

The feedback as mentioned above can be used for police investigations and criminal proceedings directly connected with money laundering and organised crime. Banks use it for employee training. Feedback in a single case remains confidential and can only be used for specific criminal proceedings for which it has been given, and for potentially related criminal proceedings. MROS, on the other hand, is authorized to provide legal assistance to FIUS in other countries having the same tasks and competences as MROS.

## [PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK STAFF IN THE EVENT OF NOTIFICATION) OF THE INSTITUTIONS OR PERSONS COVERED BY THIS DIRECTIVE ]

Financial intermediaries making a notification pursuant to Article 9 of the Money Laundering law or in accordance with Article 305ter paragraph 2 of the Penal Code and who are blocking the relative assets cannot be pursued for an infringement of financial privacy laws, nor held liable for breach of contract if they are acting diligently.

## [CONSERVATION OF RECORDS AND DOCUMENTS]

### **a) Duration**

Documents must be kept for 10 years after they become obsolete (10 years after the transaction for transactional documents; 10 years after the end of the business relationship for customer documentation).

### **b) Means of conservation**

Financial intermediaries must put on record documents relative to transactions carried out as well as customer documentation required pursuant to the Money Laundering Law so as to ensure that third party experts can obtain an objective idea concerning the transactions and business relationships. Conservation on microfiches or electronic records are possible.

## [STEPS TAKEN TO INCREASE AWARENESS OF THE PHENOMENON OF MONEY LAUNDERING (E.G.: TRAINING, INFORMATION...)]

The Swiss Financial Market Supervisory Authority's Money Laundering Ordinance requires banks to issue internal instructions in order to train personnel on how to react when faced with suspicious transactions. Self regulatory bodies meet semi-annually for an exchange of information. The MROS and ML Control Authority representatives participate in these meetings.

The Swiss Association of Compliance Officers (SACO) on its annual meetings regularly puts prevention of money laundering on the agenda and invites the Swiss Financial Market Supervisory Authority (FINMA) and the Swiss Bankers Association (SBA) to participate and/or to act as guest speakers. Self regulatory bodies, among them the SBA, also have their regular common meetings to exchange views, discuss cases and coordinate discussions with the regulator.

### [ANTI-MONEY LAUNDERING /CTF LEGISLATION]

- Proceeds of Crime Act 2002;
- Terrorism Act 2000, the Anti-Terrorism Crime and Security Act 2001, the Terrorism Act 2006;
- The Money Laundering Regulations 2007 which came into force on 15 December 2007.

### [PENALTIES IN NATIONAL LAW FOR FAILURE TO RESPECT OF THE NATIONAL PROVISIONS TO THE DIRECTIVE]

The UK's Money Laundering Regulations (2007) set out the penalties as being "a designated authority may impose a penalty of such amount as it considers appropriate on a relevant person who fails to comply with any requirement..." in the Regulations.

### [CENTRAL AUTHORITY FOR REPORTING]

The Financial Intelligence Unit in the Serious Organised Crime Agency (SOCA): SOCA was established in April 2006. It was formed from the National Criminal Intelligence Service (NCIS), and parts of HM Revenue and Customs, and the Immigration Service. In 2008 the Asset Recovery Agency merged with SOCA.

### [PERSONS RESPONSIBLE FOR REPORTING]

There are 2 separate obligations in relation to appointing individuals with responsibility for money laundering prevention.

The first obligation, which applies to all firms carrying out business which is covered by the Money Laundering Regulations, is to appoint a nominated officer who is responsible for receiving internal suspicion reports and deciding whether these should be reported to SOCA.

The second obligation only applies, with certain exceptions, to firms regulated by the UK's Regulator, the Financial Services Authority (FSA). Where the obligation applies, firms must appoint a Money Laundering Reporting Officer (MLRO) who must be given certain responsibilities. In many FSA regulated firms it is likely that the nominated officer and the MLRO will be one and the same person. A nominated officer will provide a focal point within a firm where internal suspicions are considered and decisions taken on whether to make an external

report. An MLRO will also support and co-ordinate business heads' focus on their managing of the money laundering risk in their individual business areas. He/she will also help ensure that the firm's wider responsibility for forestalling and preventing money laundering is addressed centrally. The MLRO will provide a focal point for ensuring that the firm complies with its legal and regulatory obligations. The MLRO is required to be approved by the FSA before taking up his/her appointment. The FSA also requires the appointment of a director or senior manager to take overall responsibility within a regulated firm.

[BUSINESS COVERED BY THE LEGISLATION (WHICH SPECIFIC PERSONS: NOTARIES, LAWYERS...)]

The principal legislation covers all persons. The 3<sup>rd</sup> Directive did not extend the scope of persons covered, and the 2007 Regulations cover the following activities:

- Banks, building societies, and other credit institutions;
- Individuals and firms engaging in regulated investment activities under the Financial Services and Markets Act 2000;
- Insurance companies undertaking long-term life business, including the life business of Lloyds of London;
- Issuers of electronic money;
- Money service businesses (bureau de change, cheque encashment centres and money transmission services);
- The National Savings Bank;
- Corporate service providers, company formation agents and trust service providers or managers;
- Estate agents;
- Accountants, auditors, tax advisers and insolvency providers;
- Providers of legal services that involve participation in a financial or property transaction;
- Dealers in high value goods of any description involving payments of €15,000 or more.

## [PREDICATE OFFENCES COVERED]

Prior to the Proceeds of Crime Act 2002, there was a distinction made between the laundering of the proceeds of drug trafficking and of other crimes, but the Act removed this distinction. If there is reasonable evidence that 'property' was derived from criminal conduct and that the defendant suspected this, a jury can convict without knowing what particular offence was committed. The concept of 'predicate offences' may therefore be considered redundant in the UK.

## [IDENTIFICATION]

### **a. Definition (e.g.: PEPs, beneficial owner, thresholds...)**

- (i) PEPs: in addition to the definition of PEPs in the 3<sup>rd</sup> Money Laundering Directive, the FSA provided advice in December 2006 (FSA Financial Crime Newsletter) that "the definition is complemented by a list of PEP categories. These categories provide an aid to the interpretation of the PEPs definition, but are not exclusive: firms will have to decide whether to include additional categories of PEPs on a risk-sensitive basis. For example, it may be appropriate to apply the same enhanced due diligence measures to customers who hold political functions at a sub-national level, but whose political exposure is comparable to that of similar positions at the national level. The flexibility of the definition is deliberate, and foreseen by the Directive and its implementing measures. A closed list of PEPs would be both counterproductive and against the principles of the risk-based approach".

Other guidance is contained within the JMLSG guidance ( <http://www.jmlsg.org.uk/> ). It advises that new and existing customers may not initially meet the definition of a PEP but may subsequently become one during the course of a business relationship. The firm should, as far as is practicable, be alert to public information relating to possible changes in the status of its customers with regard to political exposure. When an existing customer is identified as a PEP, enhanced due diligence must be applied.

- (ii) Beneficial owner: the JMLSG guidance states that "depending on the nature of the entity, a relationship or transaction with a customer who is not a private individual may be entered into, in the customer's own name or in that of specific individuals, or other entities on its behalf. Beneficial ownership may, however, rest with others, either because the legal owner is acting for the beneficial owner, or because there is a legal obligation for the ownership to be registered in a particular way.

In deciding who the beneficial owner is in relation to a customer who is not a private individual, the firm's objective must be to know who has ownership or control over the funds which form, or otherwise relate to the relationship and/or form the controlling mind and/or management of any legal entity involved in the funds. Verifying the identity of the beneficial

owner(s) will be carried out on a risk-based approach, and will take account of the number of individuals, the nature and distribution of their interests in the funds or the transaction and the nature and extent of any business, contractual or family.”

**b. Identification threshold amount**

Identification must be verified at the start of a business relationship or where no continuing business relationship is intended, when the sum involved is €15,000 or more, or whenever money laundering is suspected regardless of the amount.

**c. Identification at a distance (non face to face)**

The JMLSG Guidance provides information on the types of evidence that should constitute satisfactory confirmation of identity on a non-face to face basis. The Guidance also considers electronic verification and the standards that need to be met before electronic verification can be relied on.

**d. Outsourcing of identification to third parties**

The JMLSG Guidance covers both outsourcing (Chapter 2.7) and “relying on third parties” (Chapter 5). The JMLSG Guidance on outsourcing notes that “involving other entities in the operation of a firm’s systems brings an additional dimension to the risks that the firm faces, and this risk must be actively managed...”. It also notes that “In all cases, the firm should have regard to the FSA’s guidance on outsourcing.”

On ‘reliance’, the JMLSG Guidance is in relatively prescriptive terms, for example:

“For one firm to rely on verification carried out by another firm, the verification that the firm being relied upon has carried out must have been based, at least, on the standard level of customer verification. It is not permissible to rely on simplified due diligence carried out, or any other exceptional form of verification, such as the use of source of funds as evidence of identity.

Firms may also only rely on verification actually carried out by the firm being relied upon. A firm that has been relied on to verify a customer’s identity may not ‘pass on’ verification carried out for it by another firm”.

**e. Means of identification**

The Regulations do not specify what constitutes adequate evidence of identity but the JMLSG Guidance provides an interpretation of the legislative and regulatory requirements. The JMLSG Guidance goes into some detail about the different types of identification in different scenarios and sets these types against the risk based approach.

## [PRODUCTS AND TRANSACTIONS CHARACTERISED BY A HIGH/LOW RISK OF MONEY LAUNDERING]

The JMLSG Guidance identifies some questions to be considered when considering product risk:

- can the product features be used for money laundering or terrorist financing, or to fund crime?
- do the products allow/facilitate payments to third parties?
- is the main risk that of inappropriate assets being placed with, or moved from, or through the firm?
- does a customer migrating from one product to another within the firm carry a risk?

As to low risk products, HM Treasury has made it clear that Child Trust Funds should be considered in this category.

## [EXISTING GUIDELINES TO THE BANKING INDUSTRY]

UK Guidance for the financial sector is published by the Joint Money Laundering Steering Group (JMLSG) and all versions since 2001 have been approved by HM Treasury. The JMLSG currently comprises eighteen financial sector trade associations, and as such, application of its Guidance cannot be mandatory. However the procedures, which are tailored for different sectors of the financial industry, are used in the Financial Services Authority's assessment of whether a regulated firm has breached its Rules or has breached the Money Laundering Regulations. Similarly, should a case be brought before the Courts, the Courts must, in assessing guilt, have regard to whether there has been compliance with the JMLSG Guidance.

## [GENERAL FEEDBACK (NEW MODUS OPERANDI, TRENDS, REAL CASES, etc)]

The FSA has published information on specific actions taken by it against firms in the industry. Over the last three years, three banks have been fined amounts ranging from £300,000 to £1,26 million. Details of these actions can be obtained from:

[http://www.fsa.gov.uk/Pages/Library/Publications\\_by\\_date/index.shtml](http://www.fsa.gov.uk/Pages/Library/Publications_by_date/index.shtml)

In March 2008 the FSA published its findings from its 'Review of firms' implementation of a risk based approach to anti money laundering'. This is available at

[http://www.fsa.gov.uk/pages/About/What/financial\\_crime/money\\_laundering/library/reports/index.shtml](http://www.fsa.gov.uk/pages/About/What/financial_crime/money_laundering/library/reports/index.shtml)

## [PURPOSES FOR WHICH THE FEEDBACK INFORMATION MAY BE USED]

The information is only used in criminal investigations. Fiscal authorities have access to the information disclosed for use in criminal proceedings. Officers of Her Majesty's Revenue and Customs (HMRC) are located within the Financial Intelligence Unit of SOCA.

## [PROTECTION OF EMPLOYEES (INCLUDING LIABILITY OF BANK STAFF IN THE EVENT OF NOTIFICATION) OF THE INSTITUTIONS OR PERSONS COVERED BY THIS DIRECTIVE ]

There are criminal penalties within Regulation 47 for breaching the requirements of the Regulations. The JMLSG Guidance states that "in addition to imposing liability on firms, the ML Regulations impose criminal liability on certain individuals in firms subject to the ML Regulations. Where the firm is a body corporate, an officer of that body corporate, who consents or connives in the commission of an offence by the firm, or that offence (by the firm) is attributable to any neglect on his part, himself commits a criminal offence and may be prosecuted".

Section 37 of the Proceeds of Crime Act states that a disclosure made in good faith by an employee will not be treated as a breach of any restrictions on the disclosure of information.

## [CONSERVATION OF RECORDS AND DOCUMENTS]

Records evidencing that identity has been verified must be kept for at least 5 years after the relationship with the customer has ended.

Transaction records must be kept for at least 5 years after completion of the transaction.

## [STEPS TAKEN TO INCREASE AWARENESS OF THE PHENOMENON OF MONEY LAUNDERING (E.G.: TRAINING, INFORMATION...)]

The Money Laundering Regulations 2007 require that appropriate measures must be taken so that all relevant employees are made aware of the law relating to money laundering and terrorist financing, and, regularly given training in how to recognise and deal with transactions and other activities which may be related to money laundering or terrorist financing.