ROMANIA

NATIONAL OFFICE FOR THE PREVENTION
AND CONTROL OF MONEY LAUNDERING

# SUSPICIOUS TRANSACTIONS

# GUIDELINES

**UP–DATED EDITION**
**SEPTEMBER 2004**

Romanian Suspicious Transactions Guidelines have been up–dated under the TWINNING PROJECT RO02-IB/JH-08

Program financed by the European Union under PHARE

# I N D E X[1]

## *PART I – GENERAL ASPECTS*



[1] The updating of these guidelines has been coordinated and supervised by Mr. Giuseppe Lombardo, Lawyer of the Ufficio Italiano dei Cambi and Member State Project Leader. The updating has been realised by Mr. Piero Ricca, Senior Financial Analyst, Mr. Francesco Pontarelli, Financial Analysts, and by Mr. Giovanni Lupi, Lawyer, from Ufficio Italiano dei Cambi. Suggestions from the Board of the National Office and from other Romanian Institutions involved in the Project have been taken also into consideration. Mr. Ferdinando Buffoni, Pre-Accession Adviser, Ministry of Economy and Finance, ensured close scrutiny to the work. Ms. Laura Banu, acting Chief Service of the National Office, looked after the Legal Commitments and revised the text.

*h)* Interdiction of revealing and providing information to the clients in connection with money laundering, outside the legal provisions.

*Requirements for financial-control and supervision authorities*

**Chapter III - Know your Customer**

3.1. The need to know your customer

**Chapter IV - How to recognize suspicious transactions**

4.1. Suspicious transactions

4.2. Suspicious behaviour

4.3. Active participation of the reporting entity's employee

**Chapter V - Reporting suspicious transactions related to terrorism**

5.1. The international commitments

5.2. The role of financial institutions and other reporting entities

## *PART II – ANOMALY INDICATORS*

**Chapter I - Banks**

1. *Specific identification issues for banks*

   1.1. Trust, nominee and fiduciary accounts

   1.2. Client accounts opened by professional intermediaries

   1.3. Correspondent banking

2. *Suspicious categories*

   2.1. Customer behaviour

   2.2. Avoidance of reporting or record keeping requirement

   2.3.Cash transactions

   2.4. Bank accounts

   2.5. Wire transfers

   2.6. Transactions involving foreign jurisdictions

   2.7. Loan operations

# PART I - GENERAL ASPECTS

## CHAPTER I
## OVERVIEW

### *1.1. WHAT IS MONEY LAUNDERING?*

Money laundering is the activity through which the offender tries to conceal the actual origin and ownership of income derived from criminal activities.

In order to enjoy the proceeds of their predicate offence, be it drug or arms trafficking, contraband, fraudulent bankruptcy or financial/bank fraud, offenders must find a way to conceal or disguise the unlawful nature of their profits and to introduce them into the legal business system.

If successful, this activity will allow launderers to control this income and eventually will provide a legitimate cover to its source.

Money laundering is a process to convert the unlawful proceeds of a criminal activity into funds with an apparently legal source, whereby the undiscovered launderers can subsequently enjoy the fruit of their crime.

It is a dynamic three-stage process, which requires first the movement of the criminally derived funds; secondly – concealment of the money trail in order to avoid investigation; thirdly – making the money available to criminals by once again disguising the criminal and geographical source of the funds.

Definition – Law 656/2002, art. 1 letter a):

*Money laundering means the offence provided for in article 23.*

- *Violations stipulated in art. 23:*

a) conversion or transfer of property, knowing that such property is derived from criminal activity, for the purpose of concealing or disguising the illicit origin of property or of assisting any person who is involved in the commission of such activity to evade the prosecution, trial and punishment execution;

b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect top, or ownership of property, knowing that such property is derived from criminal activity;

c) acquisition, possession or use of property, knowing that such property is derived from criminal activity.

*Individuals and legal entities stipulated in art. 8:*

a) banks, branches of foreign banks and credit institutions;

b) financial institutions;

c) insurance and reinsurance companies;

d) economic agents performing gambling and pawning activities, trading in works of art, precious metals and stones, dealers, tourism operators, services providers and any other similar activities involving movement of values;

e) natural and legal persons providing legal, notarial, accounting, financial and banking advice, notwithstanding their professional secrecy legal provisions;

f) persons with attributions in the privatisation process;

g) post offices and legal persons who provide money transmission/remittance services in ROL or foreign currency;

h) real estate agents;

i) foreign exchange offices ("bureaux de change");

j) any other natural or legal person, for acts and deeds committed outside the financial and banking system.

Definition – Council Directive 91/308/EEC of 10 June 1991:

*"Money laundering means the following conduct*, when committed intentionally:

a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such 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 to evade the legal consequences of his action;

b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from criminal activity or from an act of 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 act of participation in such activity;

d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions mentioned in the foregoing paragraphs."

## ***1.2. MONEY LAUNDERING STAGES***

There is more than one way to launder money. Methods can vary from the purchase and sale of a luxury object (for instance a car or a piece of jewellery) to passing the money through a complex international network of illegal businesses and "shell"

companies (companies that exist only as legal entities without doing business or carrying on commercial activities). In the case of crimes such as drug trafficking or other offences such as smuggling, theft, blackmail etc., the proceeds are most often cash which, at the first stage, has to be introduced into the financial system, one way or another.

The traditional banking operations of setting up deposits or the money transfer and crediting systems provide a vital money laundering mechanism especially in the first stage of introducing the cash in the financial system.

Despite the variety of methods, money laundering has three stages that can include numerous transactions made by money launderers, transactions that can alert the financial institutions to criminal activities, namely:

1. Placement:

- represents “getting rid literally” of cash obtained from illegal activities, in order to separate funds from illegal sources, which could be monitored by the law enforcement agencies.

2. Layering:

- it is the process of moving money from one account to another in order to disguise their origin;

- separation of criminal proceeds from their source by creating complex layers of financial transactions designed to deceive investigative bodies and to ensure anonymity.

3. Integration:

- returning laundered funds at the disposal of the offenders, having apparently legitimate origin;

- creating an apparently legitimate justification for the criminally derived profits.

If the structuring process is successful, the integration schemes will send the results of laundering back into the economy so as they will again enter the financial system as normal and “clean” business funds.

The three basic steps may be separate and distinct stages. They can occur simultaneously or, more commonly, they may overlap. The way in which the basic steps are used depends on the laundering mechanisms available and on the requirements of the criminal organisations.

Certain weaknesses have been identified in the money laundering process, difficult to avoid by the money launderer and, consequently, easy to recognise, namely:

- placing cash in the financial system;

- taking cash across borders;

- transferring cash within and from the financial system.

## ***1.3. NEED TO COMBAT MONEY LAUNDERING***

In recent years there has been increasing recognition of the fact that fighting against organised crime is of crucial importance and that, whenever possible, offenders must be prevented from making their criminal proceeds legal by turning “dirty” funds into “clean” funds.

The ability to launder the criminal proceeds through the financial system is vital for the success of criminal activities. Those involved in such activities need to exploit the world financial system if they want to benefit from the proceeds of their conduct. The use of the financial-banking systems to launder money leads to the undermining of the individual financial institutions and in the end of the whole financial system. At the same time, the growing integration of the world financial systems and the removal of the barriers raised to free capital movement has made it increasingly easy to launder dirty money and has complicated the tracing process. The latest trends have highlighted that money launderers are more and more directing their efforts to employing also non-banking and non-financial intermediaries. Thus the fight against money laundering also reposes on the awareness of a wide range of economic entities that may well not be directly referable to the banking or financial sector.

The long-term success and stability of any economic institution depends on attracting and retaining funds earned in a legitimate manner.

Criminally obtained money is, invariably, transitory. It damages reputation and discourages the honest investor. The economic entity that gets involved in a money laundering scandal will risk prosecution and loss of good reputation on the market.

If not controlled, money laundering may undermine the efforts towards a free and competitive market and will affect the development of a sound economy.

Money laundering is a major factor of contamination for the entire economy: it can erode the integrity of the financial institutions of a country by influencing the demand for ready money, by influencing the level of the interest rate and of the currency exchange rate and, at the same time, it can generate inflation.

Through their illegal methods, offenders can invest in sectors of the economy where assets may be subsequently used as money laundering machines. Moreover, in an economy where advanced technology and globalisation allow for quick fund transfers, the lack of control over the laundering of huge amounts of money may undermine financial stability. Moreover, in a country with a precarious financial situation, taking millions, even billions of dollars annually out from the normal process of economic growth poses a real threat.

Money laundering strategies include transactions, which, in point of volume, are highly profitable and therefore attractive to legal financial institutions or other economic entities used as intermediaries by the individuals desiring to turn dirty funds into clean funds. Money laundering channels money from the illegal economy and places it, through investment, in the legal economy relying on the capacity and performance of the financial system to transfer capital and assets in huge amounts and quickly.

The expertise gained by the organised crime networks is fearsome. Consequently, the bodies and organisations authorised to fight against them should co-operate closely in

order to prevent the generalisation of the money-laundering phenomenon. If not, there is the risk, at all negligible, that the laundered money may become the “engine” of the economy and impose its own “rules,” which actually means the undermining or even the dissolution of state authority and the rule of Mafia-type arbitrariness.

## *1.4. ECONOMIC SYSTEM’S VULNERABILITY TO MONEY LAUNDERING*

Traditionally, the efforts to combat money laundering focused to a large extent on the procedures of setting up deposits by financial institutions since laundering money through this method is easily recognisable. Offenders gave a quick answer to the action taken by the financial sector in recent years acknowledging the fact that cash payments made within the financial sector may subsequently raise questions. Consequently, new means were sought to convert the criminally derived money and mix it with legitimate funds before introducing it into the financial system, rendering detection at the placement stage even more difficult. Lately, an increasing number of money laundering cases are taking ever more sophisticated forms that do not involve cash

Banks, in their capacity as suppliers of a wide range of fund transfer and lending services, can be used at all money laundering stages from placement to structuring and integration. The electronic fund transfer systems allow for quick transfers between accounts under different names and jurisdictions. Multiple and diversified transactions in accounts are used frequently as part of the money laundering process creating complex transaction layers.

In this context, sophisticate criminal organisations and “professional money launderers” want to resort to banking services in order to make use of their “dirty” funds. Through the agency of companies and individuals, these organisations generate false international commercial activities to move illegal money from one country to another using forged invoices to generate apparently legal international transfers and use fictitious operations to hide their traces. Many of the shell companies can even approach their own banks to get loans to finance such activities.

But banks do not represent the only means to launder dirty money. First of all, many financial intermediaries provide services that are similar to those traditionally offered by banks. Furthermore, in order to bypass money laundering countermeasures, those individuals desiring to launder criminal proceedings are increasingly turning their efforts to exploit the non banking sector, making use of other financial institutions (such as finance companies, brokerage houses, insurance companies, bureau de change...), as well as of non financial institutions (casinos, estate agents...). As they usually have not specialised professional expertise themselves, launderers must turn to the expertise of legal professionals, accountants, financial consultants and other professionals.

An exhaustive anti money-laundering system therefore rests on the awareness of a wide range of financial and non-financial intermediaries as well as of other economic entities that must co-operate responsibly with the authorities and respond actively against the danger of being involved in the phenomenon.

# CHAPTER II

# LEGAL COMMITMENTS

Romania has taken steps to create the appropriate legal and institutional framework to combat money laundering, thus joining the international efforts to fight drug trafficking, organised crime and money laundering that materialised, in 1989, in the initiative of the G-7 to establish the Financial Action Task Force on Money Laundering (FATF) and in the European Community Council's adopting of Directive 308/10 June 1991, including its amendments.

In this context, Romania's Parliament passed new **Law no. 656, which has been adopted in 2002,** published in the Official Gazette no. 904/12th of December 2002.
During its amendment process, the Law on the prevention and sanctioning of money laundering paid attention to the provisions stipulated in the following international legal documents:

- Directive 2001/97/EEC of the European Parliament and of the Council of the 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system from the purpose of money laundering;
- Protocol of 30 November 2000 drawn up on the basis of Article 43(1) of the Convention on the establishment of an European Police Officer (Europol Convention) amending Article 2 and the Annex to that Convention (extension of Europol's competence to money laundering in general, regardless of the type of offences from which the laundered proceeds originate);
- Council Framework Decision of the 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime;
- Joint Action on money laundering, the identification, detection, freezing or seizure of the instruments and proceeds of crime;
- Strasbourg Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime of November 1990;
- The 1988 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances ("Vienna Convention");
- UN Convention on terrorism financing suppression;
- UN Convention against transnational organized crime, signed in Palermo on 2000;
- The 8 FATF/GAFI Special Recommendations on terrorism financing;
- The 40 FATF/GAFI Recommendations – in the revised form.

**Romanian Government Decision no. 479/16th of May 2002** for the endorsement of the Rules for the organisation and operation of the National Office for the Prevention and Combating of Money Laundering was published in the Official Gazette no. 382/16th of May 2002. The Rules emphasize in art. 8 that, in fulfilling them, the Board of the National Office adopts, with a majority of votes, resolutions that have a mandatory character for natural and legal persons stipulated in art. 8 of Law 656/2002, as well as the conditions for recruiting, hiring and promoting its own staff.

**Romanian Government Decision no 1.078/08th of July 2004** for the amendments of the Rules for the organisation and operation of the National Office for the Prevention and Combating of Money Laundering, approved by the Emergency Decision no. 479/2002, published in the Official Gazette no. 382/16th of May 2002. Under this

Decision, it is stipulated that the Board and Departments functions will be set up through the Prime Minister Order, at the National Office President proposal, and for the functions of others compartments, through the Order of the National Office President, under the law.

**Resolution of the Board of the National Office for the Prevention and Control of Money Laundering no. 657/20th of December 2002**, published in Official Gazette no. 2/7th of January 2003, on the approval of the forms and contents of the following report: Suspicious Transactions Report, Currency Transaction Report for cash deposits and withdrawals in excess of the equivalent of EUR 10,000, and Cross-Border Transfers Report.

## *REPORTING ENTITIES OBLIGATIONS IN KEEPING WITH LAW 656/2002 ON PREVENTION AND CONTROL OF MONEY LAUNDERING*

### a. Requirement for client's identification

**Art. 9**

**(1)** The persons provided in article 8 have the obligation to establish the identity of their customers, when entering into business relations, opening accounts or offering services.

**(2)** The identification requirement applies also to any transactions, other than those provided in the paragraph 1, whose minimum value is equivalent to EUR 10,000, irrespective whether the transaction is carried out in a single operation or in several linked operations.

**(3)** As soon as there is any information that the transaction has the purpose of money laundering, the customers identification shall be made, even if the value of the transaction is lower than the minimum limit provided in para (2).

**(4)** Where the sum is not known at the time when the transaction is accepted, the natural or legal person having the obligation to identify the customers, shall immediately proceed with their identification, as soon as it knows the value of the transaction and when it has been established that the minimum limit provided in para (2)has been reached.

**(5)** The provisions of para 1-4 shall apply also to all transactions involving persons who are not physically present for identification purposes (non - face - to - face operations).

**Art. 10**

**(1)** Identification data regarding customers shall include:

a) for natural persons: data mentioned in the identity documents provided by the law;

b) for legal persons: data mentioned in the incorporation documents provided by the law, as well as the proof that the natural person performing the transaction is the legal representative of the legal person.

**(2)** for foreign legal persons, when opening bank accounts, there shall be requested those documents indicating the identity of the company, the address, the type of company, the place of incorporation, the special power of attorney for the person representing the company in the transaction, as well as a translation in Romanian of the respective documents, certified by a public notary.

**Art. 11**
In cases where there are information referring to the customers provided in art. 9 and 10, that the transaction is not performed in their own name, the legal persons mentioned in art. 8 shall take measures in order to obtain information about the real identity of the person on whose interest or behalf are acting these customers, including information from the Office.

**Art. 12**
**(1)** Identification requirements shall not apply to insurance and reinsurance companies provided in article 8, concerning life insurance policies, if the insurance premium or the annual rates are lower or equal to the equivalent in ROL of EUR 1,000 or if the single insurance premium paid does not exceed the equivalent in ROL of EUR 2,500. If the periodical premium rates or the amounts to be paid in any given year are higher or will be increased so as to exceed the EUR 1,000 threshold or respectively EUR 2,500 equivalent in ROL, the identification of the customers shall be required.
**(2)** Identification requirements shall not be compulsory for the subscription of insurance policies issued by the pension funds, obtained by virtue of a labor contract or due to the profession of the insured person, on condition that such policy may not be redeemed before maturity and may not be used as a guarantee or collateral in order to obtain a loan.

**Art. 28**
The identification of customers, in accordance with art.9, shall be made starting with the date of entering into force of this Law.

**b. Reporting entities requirement on setting up of internal procedures for prevention of money laundering**

**Art. 16**
**(1)** The legal persons provided in art. 8 shall establish adequate procedures and methods of internal control, in order to prevent and combat money laundering, and shall ensure the training of their employees on detecting the transactions that could be related to money laundering and on taking the immediate measures in such situations.
**(2)** The Office shall participate to the special training programmes for the representatives of the persons provided in art.8.

**c. Reporting entities requirement on designation of compliance officers**

**Art. - 14**
**(1)** The legal persons provided in art. 8 shall appoint one or more persons having responsibilities in the enforcement of this law, whose names shall be notified to the Office, together with the nature and limits of the mentioned responsibilities.

**d. Reporting obligation to the Office of:**

- Suspicious transactions, before and after their performing;
- Cash deposit/withdrawal operations over the threshold of Euro 10.000;
- External transfers over th threshold of Euro 10.000.

**Art. 3**

**(1)** As soon as an employee of a legal or a natural person of those stipulated in article 8, has suspicions that a transaction, which is on the way to be performed, has the purpose of money laundering, he shall inform the person appointed according to art. 14, para (1), who shall notify immediately the National Office for Prevention and Control of Money Laundering, hereinafter referred to as "the Office". The Office shall confirm the receipt of the notification.

**(6)** The persons provided in article 8 or the persons designated in accordance with art. 14 para (1) shall report to the Office, within 24 hours, about all cash transactions performed, in ROL or in foreign currency, whose minimum limit represents the equivalent of Euro 10,000, irrespective whether the transaction is carried out in a single operation or in several linked operations.

**(7)** The provisions under paragraph (6) shall also apply to cross-border transfers to/from accounts, for amounts exceeding the equivalent of Euro 10,000.

**(9)** The Board of the Office shall decide on the reporting form to be used for the operations provided in paragraphs (1), (6) and (7), within 30 days from the entering into.

**Art. 4**

If the persons provided in article 8 have knowledge that a transaction, for which they have received instructions to perform it, has the purpose of money laundering, they may perform the transaction without a prior notification to the Office, if the transaction must be carried out immediately or, if by not performing it, the efforts to trace the beneficiaries of such money laundering suspect operation could be hampered. These persons have the obligation to notify the Office immediately, but not later than 24 hours, about the performed transaction, specifying the reason for non-compliance to the provisions of art. 3.

**Art. 7**

Information supplied in good faith, in accordance with the provisions of the art. 3-5, by the persons provided in article 8 or by the persons appointed in accordance with art. 14 para (1), may not result in disciplinary, civil or penal liability of these persons.

**Art. 14**

**2)** The persons appointed according to the paragraph 1 shall be responsible for the performance of the tasks established for the enforcement of this law.

**Art. 15**

The persons designated according to the art. 14 paragraph (1) and the persons provided in art. 8 shall draw up a written report for each suspicious transaction, in the form established by the Office, which shall be immediately submitted to the Office.

**e. Interdiction of performing transactions during the suspension period communicated by the Office**

**Art. 3**

**(2)** If the Office considers as necessary, it may decide to suspend the transaction for 48 hours, based on the existing reasons.

**(4)** Within 24 hours, the Office must notify the persons provided in art. 8, the decision to suspend the transaction or the disposition to extend the period of

suspension, authorised by the General Prosecutor's Office by the Supreme Court of Justice.

**(5)** If the Office didn't make the notification, within the period provided in para (4), the persons referred to in art. 8, may carry out the transaction.

**f. Requirement of all institutions to communicate all requested data and information on deadline for accomplishing the Office functions.**

**Art. 5**

**(1)** The Office may require to the persons referred to in art.8, as well as to the competent institutions, data and information necessary to perform its competences provided by the Law. The information related to the notifications received according to the art. 3 and 4 is subject to confidentiality.

**(2)** The persons provided in art. 8 shall submit to the Office the required data and information, within 30 days, from the date of receiving the request.

**(3)** The professional secrecy related to the entities mentioned in article 8 is not opposable to the Office.

**g. Requirement for keeping documents related to the identification of the client and to the transactions under the Law no. 656/2002**

**Art. 13**

**(1)** In each case when the identity is required according to the provisions of this Law, the legal or natural person provided in article 8, which has the obligation to identify the customer, shall keep a copy of the document, as identity proof or identity references, for a period of 5 years, from the date when the relationship with the customer ends.

**(2)** The persons referred to in art. 8 shall keep the secondary or operative records and the records of all financial transactions subject to this law, for a period of 5 years from the performance of every transaction, in an appropriate form, in order to be used as evidence in Court.

**h. Interdiction of revealing and providiong information to the clients in connection with money laundering, outside the legal provisions**

**Art. 18**

**(2)** The persons provided in art. 8 and their employees are obliged not to disclose the information they are holding, related to money laundering, except under legal conditions, and may not warn their customers regarding the notification to the Office.

**(3)** The use for personal purposes of the information received by the Office's personnel and by the employees of the persons provided in art. 8, during the activity and after its ceasing, is forbidden.

***REQUIREMENTS FOR FINANCIAL-CONTROL AND SUPERVISION AUTHORITIES***

**Art. 17**

**(1)** The authorities with financial control powers, according to the law, and those with prudential supervision tasks on the persons referred to in art.8, shall verify and

control the enforcement of the present law, within the performance of their legal duties, and if there are suspicions of money laundering or infringements to the provisions of the this law, they shall immediately notify the Office.

**(2)** The Office may perform joint checks and controls on the persons provided in art. 8, together with the authorities mentioned in para (1).

# CHAPTER III

# KNOW YOUR CUSTOMER!

## ***3.1. THE NEED TO KNOW YOUR CUSTOMER***

### KYC for Credit Institutions

Knowing the customer is vital to any credit institution, as it lays the foundation for all future activities based on the credit institution -customer relationship. When a business relationship is established with a customer the nature of the business should be defined to clearly know what a normal activity should be.

To be able to analyse whether a transaction is suspicious or not, credit institutions must know exactly the legitimate businesses of their customers.

The need to know the customers does not result only from the provisions of the anti-money laundering Law; it should be a fundamental concern since the proper course of the credit institution's activity depends on the consistent application of this requirement.

The procedures a credit institution adopts in order to comply with anti-money laundering legislation inevitably duplicate prudential fraud-prevention measures, measures that pursue the protection of both the bank and its customers.

Customer due diligence should be a continuous process, a must for good banking practice in order to identify the transactions that can be related to illegal activities. To this end internal norms must be adapted and operating and control procedures must be adjusted for a better assessment of transactions and of the relationship with the customers.

In order to identify and isolate operations pursuing money laundering, the credit institutions must establish their relationship with their customers in a spirit of trust and co-operation while customers should ensure a transparency of their business handled by credit institutions.

The credit institution officer must have very good knowledge of his/her customer, his/her economic conditions and his/her financial needs.

Opening an account is the result of a thorough evaluation of the customer. This should make the potential customer seek acceptance by the credit institution not only by proving his/her identity but also by supplying proof of personal integrity as a prerequisite for a profitable and fair relationship.

In conformity with the above, customers must be informed about the requirements and objective of the anti-money laundering law, about the fact that they are called upon to co-operate by accepting pre-established identification procedures.

Acceptance of these rules of conduct is compulsory for both the customers applying for loan and for those that make deposits thus introducing their gains in the financial system.

KYC procedures for credit institutions have particular relevance to their safety and soundness. They help to protect credit institutions' reputation and the integrity of banking systems by reducing the likelihood of credit institutions becoming a vehicle for or a victim of financial crime and suffering consequential reputation damage Furthermore they constitute an essential part of sound risk management.

Therefore the inadequacy or absence of KYC standards can subject credit institutions to serious customer and counterpart risks, especially reputation, operational, legal and concentration risks. It is worth noting that all these risks are interrelated.

In this respect credit institutions should have adequate policies, practices and procedures that promote high ethical and professional standards and prevent them from being used by criminal elements in place. Certain key-elements should be included by credit institutions in the design of KYC programmes. Such essential elements should include:

- a customer acceptance policy,
- customer identification procedures,
- up-to-date record-keeping procedures,
- on-going monitoring of accounts and transactions, in order to detect the suspicious transactions, and the procedure of reporting them,
- guidance of conducting the transactions in and/or from the jurisdictions having non-adequate regulations in the anti-money laundering field,
- procedures and control systems of the KYC programme's implementation and evaluation,
- on-going employee-training programme so that credit institutions employee/staff is adequate trained in KYC procedures.

Credit institutions should not only establish the identity of their customers, but should also monitor account activity to determine those transactions that do not conform with the normal transactions for that customer or type of account.

A credit institution's customer acceptance procedure should including a description of the types of customer that are likely to pose a higher than average risk to a bank. In preparing such policies, factors such as customers' background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators should be considered. For example, the policies may require the most basic account-opening requirements for a working individual with a small account balance.

It is important that the customer acceptance policy is not so restrictive that it results in a denial of access by the general public to banking services, especially for people who are financially or socially disadvantaged. On the other hand, quite extensive due diligence would be essential for an individual with a high net worth whose source of funds is unclear. Decisions to enter into business relationships with higher risk customers, such as politically exposed persons (see section 2.2.3 below), should be taken exclusively at senior management level or, if the case, at the executive management level in accordance with the responsibilities given.

A credit institution should establish a systematic customer identification procedure for verifying of the new customers and those acting on their behalf, and shall enter a business relationship until the identity of a new customer is satisfactory established. Credit institutions should document and enforce policies for identification of customers and those acting on their behalf. Special attention should be exercised in the case of non-resident customers and in no case should a bank short-circuit identity procedures just because the new customer is unable to present himself for interview.

The credit institution should always ask itself why the customer has chosen to open an account in a foreign jurisdiction. To ensure that records remain up-to-date and relevant, there is a need for credit institutions to undertake regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated. However, if a credit institution becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.

Credit institutions should develop “clear standards on what records must be kept on customer identification and individual transactions and their retention period”. Such a practice is essential to permit a credit institution to monitor its relationship with the customer, to understand the customer’s on-going business and, if necessary, to provide evidence in the event of disputes, legal action, or a financial investigation that could lead to criminal prosecution.

In each case reputation risk may arise if the credit institution does not diligently follow established KYC procedures. Therefore on-going monitoring is an essential aspect of effective KYC procedures. Credit institutions can only effectively control and reduce their risk if they have an understanding of normal and reasonable account activity of their customers so that they have a means of identifying transactions which fall outside the regular pattern of an account’s activity. Without such knowledge, they are likely to fail in their duty to report suspicious transactions to the appropriate authorities in cases where they are required to do so. The extent of the monitoring needs to be risk-sensitive. For all accounts, credit institutions should have systems in place to detect unusual or suspicious patterns of activity. Certain types of transactions should alert credit institutions to the possibility that the customer is conducting unusual or suspicious activities. They may include transactions that do not appear to make economic or commercial sense, or that involve large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer. Very high account turnover, inconsistent with the size of the balance, may indicate that funds are being “washed” through the account.

Identification procedures, information about the activity and the purpose of the clients, and moreover on-going monitoring can play an important role also in case of business relations introduced through other credit institutions, correspondence or other means, as telephone, e-mail or Internet. The increasing use of financial channels based on long-distance communications (Internet Banking, Home Banking), the development of means of payments as electronic money-cards usable on Internet could represent new opportunities for money-launderers: therefore it is important to monitor adequately the use by the clients of such channels and means of payments.

Examples of suspicious activities can be very helpful to credit institutions and should be included as part of a jurisdiction's anti-money-laundering procedures and/or guidance.

Know your customer procedures previously mentioned are suited also for the financial institutions under the Law no. 656/2002, which are required to identify their clients.

# CHAPTER IV

# HOW TO RECOGNISE SUSPICIOUS TRANSACTIONS

## *4.1 SUSPICIOUS TRANSACTIONS*

Since there is a virtually unlimited number of types of transactions a money launderer can engage in, it is difficult to define what a suspicious transaction is. The suspicious character of the transaction devolves from the unusual way it is performed in relation to the current activities of a customer. Suspicions arise from clues or suppositions about a transaction linked to money laundering. Suspicion is personal and subjective, and generates mistrust in the person or persons performing the transaction, and doubt regarding the correctness and lawfulness of facts or of the honest intentions of the person involved.

In case of lasting client relation, such as the bank/customer type of relationship, a suspicious transaction will be one that does not corresponds to the data of the customer, with his/her personal activities, with the terms of a legal deal or with his/her routine transactions.

Generally speaking, the first and the most efficient method of recognising a suspicious transaction is to have enough knowledge about the customer and about his/her business so as to be able to recognise a suspicious transaction or a series of suspicious transactions.

As a rule, employees of reporting entities are more likely to recognise money laundering if a customer behaves unusually

- In the starting phase of a durable relationship (e.g. when opening an account)
- If transactions are not transparent.

The questions a financial institution or any other reporting entity should answer in order to establish whether the transaction with a current customer is suspicious or not are:

- Is the customer willing to provide personal background information when opening an account or purchasing monetary instruments or when enquiring or purchasing the services?
- Does the scope of the transaction correspond to the normal known activities of the customer?
- Is the transaction normal in the context of the customer's business or personal activities?
- When the transaction is international, has the customer an apparent reason to conduct a piece of business that involves financial-banking institutions in another country?

This information may not be available for occasional customers or for those types of activities, which are no characterised by lasting client relationship. In this case the reporting entity must adopt a more cautious attitude and the evaluation of the transaction must focus primarily on the objective features of the transactions and on the customers behaviour.

## ***4.2. SUSPICIOUS BEHAVIOUR***

Reporting entities are expected to evaluate transactions not only on the basis of their objective features (see the following chapters for specific indicators) but also in the basis of the customer's subjective profile and behaviour. Examples of abnormal customer conduct may be the following:

1. Customers who refuse or are reluctant to provide the information needed to carry out transactions or that who provide false or misleading information.

A customer/company that is reluctant to reveal details about its activities or to provide financial statements, or whose financial statements are noticeably different from those of similar businesses.

A customer who presents unusual or suspicious identification documents that the bank cannot readily verify.

Customers who ask to cancel or restructure a transaction where, as originally set up, it would have involved reporting, identification, registration or additional inquiries by the reporting entity.

Customers who avoid direct contacts with the R.E.'s employees or collaborators giving frequent mandates or proxies in a manner that appears unjustified.

Clients who, without plausible justification, use an intermediary or an intermediary's collaborator located far from their place of residence or activity

Clients who carry out large transactions using cash or bearer instruments when they are known to have recently been investigated in connection with penal proceedings.

Customers in economic difficulties who carry out large transactions without providing a plausible explanation of the source of the funds:

- customers who unexpectedly extinguish all or part of their debts;
- customers who ask to take out insurance policies that involve the payment of large premiums;
- customers who buy the R.E's services or products for large amounts.

Customers who ask to carry out transactions in unusual ways, especially if highly complex or for large amounts or with an illogical configuration.

The customer's background is inconsistent with its business activities.

A customer attempts to induce the employee to commit a breach of duty (e.g. to not file any required record keeping or reporting forms).

A customer always appears accompanied by an unknown third person (this gives the impression that the customer is supervised or guarded).

## ***4.3. ACTIVE PARTICIPATION OF THE REPORTING ENTITY'S EMPLOYEES***

- Unusual changes in the employees' conduct such as prodigal lifestyle, avoiding taking holidays, property above his/her possibilities based on regular income.
- Deliberate violation by the employee of internal anti-money laundering procedures or regulations.
- Intentional circumvention of approval authority by splitting transactions.
- Refusal by the employee to report obvious suspicious transactions.
- Customer informed he is under suspicion of possible money laundering activities.
- Customer requests to work exclusively with a certain employee.

# CHAPTER V

# REPORTING SUSPICIOUS TRANSACTIONS RELATED TO TERRORISM

## *5.1. INTERNATIONAL COMMITMENTS*

After the tragic events of September 11th, 2001 decisions were taken at international level in order combat the terrorism financing by cutting off its financial sources and by denying terrorists and their associates the access and the abuse of the financial systems. In this context FATF adopted in October 2001 Eight Special Recommendations related to:

1. Ratification and implementation of UN instruments (in particular the 1999 UN International Convention for the Suppression of the Financing of Terrorism and the five Resolutions taken by UN Security Council in this context from 1999 to 2001).

2. Criminalisation of terrorism financing.

3. Effectiveness of countries' laws and procedures to freeze or confiscate terrorist funds or other assets of persons designated by UN relevant resolutions.

4. Mandatory requirement (by law or other regulation) for financial institutions to report to FIU when it suspects or has a reasonable ground to suspect that funds are linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations or those who finance terrorism.

5. Reinforcement by countries of international co-operation in order to permit the exchange of information regarding terrorism finance (trough legal assistance mechanisms and through other mechanisms like the exchanges between FIUs and other agencies) and to permit and facilitate the extradition.

6. Requirement for the control (licensing or registration) of persons or legal entities providing money and value transmission services, including the use of informal systems or networks.

7. Requirement for financial institutions (in particular) to include originator information on wire transfer sent/received, to maintain such information at each stage of the transfer process and to monitor funds transfers in particular when complete originator information is not available.

8. Review of the legal regime of entities, in particular no-profit organisations, to prevent their misuse for terrorist financing purposes.

As regards to the international commitments Romania has ratified and implemented the 1999 UN International Convention For the Suppression of the Terrorism Financing and carried out the UN resolutions for the prevention and suppression of the phenomenon, particularly the UN Security Council Resolution 1373.

As consequence of that in the Emergency Ordinance no. 141/25 October 2001 on sanctioning certain acts of terrorism and actions of infringement of public order was defined the concept of "act of terrorism" and established the related penalties. Emergency Ordinance no. 159/2001 criminalizes terrorism financing, provides measures about the freezing of assets for natural and legal persons mentioned in the Un Lists; moreover, the Ordinance established the involvement of a group of Ministries and Authorities (included the National Office for the Prevention and Control of Money Laundering) in the elaboration, up-dating and implementation of the list of natural and legal persons suspected of financing terrorism. In particular, banks and other financial institutions, in case of operations made by or on behalf of such persons, must go through a pre-authorisation procedure of the National Bank of Romania, the National Commission for the Securities and the Supervisory Commission of the Insurances.

## ***5.2 THE ROLE OF FINANCIAL INSTITUTIONS AND OTHER REPORTING ENTITIES***

Terrorist financing has different goals with respect to money laundering, as the final scope is not always the gain of a profit and the source of funding and financing is often "legitimate"; in any case both money launderers and terrorist organisations move money, in particular from a country to another, and aim to hide their financial tracks.

As consequence of that, and a part from the case of operations referable to persons mentioned in the lists, the role of banks and other financial institutions - as in particular bureaux de change, stockbrokers, insurance companies and money remittance service - is essential to face terrorism financing.

The means are the same used to face money laundering: KYC standard rules, on-going monitoring of specific transactions (as money remittance and wire transfers) and of clients accounts who operate with counterparts located in or originating from countries at risk of terrorism.

Banks and other financial intermediaries are especially requested to pay attention to no-profit and charitable organisations and their activities and related operations as

- existence of different no-profit organisations with unexplained links (organisations sharing the same address, same managers or personnel or transferring money to each other or using the same gatekeeper in their relation with the financial system); no-profit organisations operating in various areas or countries under different names;

- large amounts of money (in particular cash) declared as collected from the public or from specific ethic or religious communities; the amounts appear inconsistent with the purpose and the activity of the no-profit organisation or with the community where the funds were apparently raised;

- sudden increase in the frequency and amounts of financial transactions for the account of a no-profit organisation, or the inverse, that is the no-profit organisation holding funds in its account for a very long period;

- operations or transactions to or from high-risk countries; operation of the same kind performed on their own behalf by no-profit organisations' directors originating form such countries.

The identification of transactions where funds are suspected to be linked or related to terrorism has as consequence the transmission of a report to the competent Authorities.

Other types of professions, business or business activities falling under anti-money laundering reporting obligations should consider the implications for their activities deriving from the laws, regulations and guidelines issued with the scope to combat the terrorism financing.

# PART II – ANOMALY INDICATORS

## CHAPTER I - BANKS

### 1. SPECIFIC IDENTIFICATION ISSUES FOR BANKS

As referred in Part I, Chapter III (KYC) all banks should have adequate procedures in place that help the bank from being used for money laundering purposes. Certain key elements such as customer acceptance policies, customer identification requirements, on-going monitoring of high risk accounts and risk management should be included, when designing a Know Your Customer –program.

In any case banks need to obtain all information necessary to establish to their full satisfaction the identity of each new customer and the purpose and intended nature of the business relationship. Beside the general identification requirements which are mentioned in Part I, Chapter III the nature of banking business can confront banks with specific identification issues such as:

#### ***1.1. Bank accounts***

Bank accounts can be used to circumvent customer identification procedures. It is essential that the true relationship is understood. Banks should establish whether the customer is taking the name of another customer, acting as a "front", or acting on behalf of another person as trustee, nominee or other intermediary. If so, a necessary precondition is receipt of satisfactory evidence of the identity of any intermediaries, and of the persons upon whose behalf they are acting, as well as details of the nature of the trust or other arrangements in place. Specifically, the identification of a trust should include the trustees, settlers/grantors and beneficiaries.

#### ***1.2. Client accounts opened by professional intermediaries***

When a bank has knowledge or reason to believe that a client account opened by a professional intermediary is on behalf of a single client, that client must be identified. Banks often hold “pooled” accounts managed by professional intermediaries on behalf of entities such as mutual funds, pension funds and money funds. Banks also hold pooled accounts managed by lawyers or stockbrokers that represent funds held on deposit or in escrow for a range of clients. Where funds held by the intermediary are not co-mingled at the bank, but where there are “sub-accounts” which can be attributable to each beneficial owner, all beneficial owners of the account held by the intermediary must be identified.

Where the funds are co-mingled, the bank should look through to the beneficial owners. Banks should accept such accounts only on the condition that they are able to establish that the intermediary has engaged in a sound due diligence process and has the systems and controls to allocate the assets in the pooled accounts to the relevant beneficiaries. Where the intermediary is not empowered to furnish the required

information on beneficiaries to the bank, for example, lawyers bound by professional secrecy codes, then the bank should not permit the intermediary to open an account.

### ***1.3. Correspondent banking***

Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Used by banks throughout the world, correspondent accounts enable banks to conduct business and provide services that the banks do not offer directly. However, if banks fail to apply an appropriate level of due diligence to such accounts, they expose themselves to the range of risks, and may find themselves holding and/or transmitting money linked to corruption, fraud or other illegal activity.

Therefore banks should gather sufficient information about their respondent banks to understand fully the nature of the respondent's business. Factors to consider include: information about the respondent bank's management, major business activities, where they are located and its money-laundering prevention and detection efforts; the purpose of the account; the identity of any third party entities that will use the correspondent banking services; and the condition of bank regulation and supervision in the respondent's country. For their part, respondent banks should have effective customer acceptance and KYC policies.

Banks should pay particular attention when continuing relationships with respondent banks located in jurisdictions that have poor KYC standards or have been identified as being "non-cooperative" in the fight against anti-money laundering.

## 2. SUSPICIOUS CATEGORIES

There are ten basic categories described below of activities and transactions that warrant close scrutiny.

The list is illustrative and while large is not comprehensive. It can be interdependences. There may be numerous reasons why a transaction, which does not appear on this list, might be suspicious.

A. Customer behaviour

B. Avoidance of reporting or record keeping requirements

C. Laundering money using cash transactions

D. Laundering money using bank accounts

E. Laundering money using wire transfers

F. Laundering money using foreign operations

G. Laundering money through loan operations

H. Laundering money using investment related transactions

I. Laundering money using documentary business and guarantees

### ***2.1. Customer behaviour***

In addition to the examples regarding the suspicious behaviour mentioned in the General Part, the following patterns may specifically be observed in the banking sector:

- A customer who is unwilling to provide personal background information when opening an account or purchasing monetary instruments above a specified threshold.

- A potential borrower is reluctant or refuses to state a purpose for a loan or the source of repayment, or provides a questionable purpose and/or source.

- A customer's business changes ownership and the background of the new owners is inconsistent with the nature of the customer's business, or the new owners are reluctant to provide personal and financial background information.

- For large businesses or corporations, financial statements are not prepared by an accountant.

- A customer who has no record of past or present employment but makes frequent large transactions.

- A customer persistently urges the bank employee to conclude a transaction quickly and unbureaucratically, without there being an understandable reason for such haste (time pressure!)

- A customer announces incoming payments, which later are not credited to the originally designated account.

- A customer avoids personal contact with the bank, with communication taking place only via telefax or telex; in some cases, the customer will name third parties (trustees) as persons entitled to dispose of the account in order to avoid contact.

- A customer does not wish to have account statements sent to him/her and/or picks up mail/account statements at the bank only once or twice a year or not at all.

- A customer does not want to indicate his/her previous or other bank(s).

### ***2.2. Avoidance of reporting or record keeping requirements***

- A customer who is reluctant to provide the information needed for a mandatory report, to have the report filed, or to proceed with a transaction after being informed that the report must be filed.

- Any individual or group that coerces or attempts to coerce a bank employee to not file any required record keeping or reporting forms.

### ***2.3. Laundering money through cash transactions***

- Exchange of large amounts of cash from one currency into another with no obvious economic purpose particularly when the customer aims at doing this frequently.

- Exchange of large quantities of banknotes of small denominations for banknotes of large denominations.

- Unusually substantial cash deposits and withdrawals made by a customer (individual or legal entity) whose activities usually involved the use of cheques or other non-cash payment instruments.

- Substantial increase of cash deposits or hard currency transactions of a customer with no apparent reason, particularly if such amounts are subsequently transferred, within a short period of time to a destination that normally cannot be associated with the customer.

- Unusually large cash deposits and withdrawals made by a customer who normally uses a current account.

- Retail business has dramatically different patterns of cash deposits than other similar businesses in the same general location.

- Currency transactions from businesses that do not normally generate currency.

- Cash deposits in several accounts, in small (negligible) amounts but bringing the total to a significant sum (smurffing).

- Use of multiple monetary instruments to pay a single entity, especially when no apparent business purpose would necessitate use of multiple instruments.

- Customers who, together and simultaneously, use different counters to make big cash transactions or foreign currency transactions.

- A customer (e.g. a one location store owner) who makes several deposits on the same day at different cashiers desks or branches.

- Structured currency transactions under a specified threshold (including same day/multiple day; same bank/different branches; different banks (if known); or the deposit or withdrawal of currency transactions before and after a financial institution's cut-off period so that the combined transaction is treated as if it had occurred over two days).

- Use of high volume, low denomination monetary instruments for normal commercial transactions.

- Cash withdrawals and deposits of unusually large amounts from/to the current account of a legal entity, which normally uses non-cash methods of payment.

- Customers who constantly deposit cash to cover bills of exchange, money transfers or other negotiable and easily sellable payment instruments.

- Transfers of large amounts of money abroad or from abroad with cash payment instructions.

- Frequent cash deposits made in the account of a customer by third parties without an apparent link to the account holder.

- Repeated transfers of large amounts abroad with the instruction to pay the money to the recipient in cash.

- Use of night safe facilities for large cash deposits.

- Cash deposits that contain counterfeit bills or altered instruments.

- Cash withdrawals immediately after cash deposits operations are made in the account.

- Repeated withdrawals from the few branches of the same credit institution.

- Cash withdrawals from the account just before the account to be closed or cash withdrawals from an account where were unusually transfered large amounts from a domestic credit institution or from abroad.

- Cash deposits immediatelly followed by transfering the total amount to other account from a domestic credit institutions or from abroad.

- Opening deposit accounts in the few branches of the same credit institution without any apparent purpose.

- Large cash deposits performed by power of attorney person in the account of his client.

- Frequent cash withdrawals having the same value (over the threshold of ROL 30.000.000), with the motivation ”payments to natural persons” or „different payments”.

- Frequent cash withdrawals without any motivation to be in concordance with the activity declared by the company.

- Cash deposits made by the associates/administrators into the company´s account, followed by repeated cash withdrawals motivated as ”paying back fo the loan”.

### ***2.4. Laundering money through bank accounts***

- Use of accounts that do not reflect normal banking or commercial activities, only for deposits or withdrawals.

- Corporate account(s) where deposits or withdrawals are primarily in cash rather than checks.

- Large withdrawals of cash from an account, previously dormant or from an account, which unexpectedly received a substantial amount from other account opened in a domestic bank or from abroad.

- Business account history shows little or no regular, periodic activity; account appears to be used primarily as a temporary repository for funds that ultimately are transferred abroad.

- Frequent and substantial transfers of funds (or depositing of other financial instruments) that cannot be clearly identified as having an economic reason.

- Substantial increase, with no apparent reason, of a customer’s turnover as reflected by the activity of his/her accounts.

- Concurrent transfers of large amounts and withdrawal of cash amounts the same day or the previous day, when the customer’s situation does not justify such an activity.

- Use of an account only as a temporary deposit of funds, which, eventually, will be transferred to other accounts abroad.

- Opening by a customer of a large number of accounts with the branches of the same bank or with different banks and repeated transfers of large amounts of money among these accounts.

- Existence of several accounts of a customer with several banks in the same town, when these accounts are supplied with large amounts of money, prior to a request for progressive transfers of funds.

- Small cash deposits in a customer's account followed by immediate transfer to an account with another bank.

- Repeated opening and closing of accounts in the name of the same customer or of a member of his/her family, without a plausible reason.

- Frequent receipt by a customer of large amounts of money from countries usually associated with the production, manufacturing or sale of drugs.

- Crediting and debiting of an account the same day or the previous days.

- A customer makes large and frequent large cash deposits and maintains high balances but does not avail itself of other services, such as, loans, letters of credit, etc.

- Supplies to an account by cheques issued by third parties in large amounts endorsed in favour of the customer.

- Suspicious movements of funds out of one bank into another bank and then back into the first bank. For example, the following scheme has been observed: 1) purchasing cashier's checks from a bank, 2) opening up a checking account at another bank, 3) depositing the cashier's checks into this checking account, and then, 4) wire transferring the funds out of the checking account back to an account at the first bank from which the cashier's checks were originally issued.

- Periodical transfers from client´s personal account to the accounts of credit institutions situated in high risk countries.

- Cash deposits in several accounts having the value under the threshold, followed by the transfer of money to a single account and from there to abroad.

- Payments or incoming payments having no apparent connection to an existing commercial legal contract.

- Transfers of large amounts on behalf of the client without any motivation or any reasonable justification.

- Transfers of funds from high risk countries, where the client has apparentlly no commercial activity or where there is no concordance with the commecial activity declared by the client or his background.

- Transfers of the same amounts from the same sender, followed by the cash withdrawals of the transfered amounts.

- Transfers of large amounts, followed by cash withdrawals of the transfered amounts, having the motivation „paying back of the loan".

- Repeated transfers of funds (usually having the same value), through the accounts of involved companies.

***2.5. Money laundering through wire transfers***

- Frequent transfers from the account of a legal entity to the account of an individual without any reference to the nature of transfers.

- Unusual transfer of funds between related accounts or accounts that involve the same principal or related principals.

- Sending or receiving frequent of large volumes of wire transfers to and from offshore institutions.

- A customer maintains multiple accounts, transfers money among the accounts, and uses one account as a master account from which wire funds transfers originate into which wire transfers are received. (A customer deposits funds into several accounts, usually in amounts below a specified threshold, and the funds are then consolidated into one master account and wired outside of the country.)

- Instructing the bank to transfer funds abroad and to expect an equal incoming wire transfer from other sources.

- Regularly depositing or withdrawing large amounts by wire transfers to, from, or through countries that are known sources of narcotics or whose bank secrecy laws facilitate the laundering of money.

- Wiring cash or proceeds of a cash deposit to another country without changing the form of the currency.

- Receiving wire transfers and immediately purchasing monetary instruments prepared for payment to a third party.

- A customer sends and receives wire transfers (to/from financial heaven countries), particularly if there is no apparent business reason for such transfers or such transfers are not consistent with the customer's business or history.

- A business customer uses or evidences a sudden increase in wire transfers to send and receive large amounts of money, internationally and/or domestically, and such transfers are not consistent with the customer's history.

- An account that receives many small incoming wire transfers or makes deposits using checks and money orders, and almost immediately wire transfers almost all of the account balance to another city or country, when such activity is not consistent with the customer's business or history.

- A customer pays for large (international and domestic) wire transfers using multiple monetary instruments drawn on several financial institutions.

- A non-customer or a customer receives or makes outgoing wire transfers involving currency amounts just below a specified threshold, or that involve numerous bank or travellers checks.

- A non-customer or a customer receives incoming wire transfers under instructions from the bank to "Pay Upon Proper Identification", or to convert the funds to cashier's checks and mail them to the customer or non-customer, when

    - The amount is very large;

- The amount is just under a specified threshold;
- The funds come from a foreign country; or
- Such transactions occur repeatedly.

- A customer or a non-customer arranges large wire transfers out of the country, which are paid for by multiple cashier's checks or other payment instruments (possible just under a specified threshold).

- A customer experiences increased wire activity when previously there has been no regular wire activity.

- Instructions to transfer funds abroad without a plausible reason for payment.

- Transfers to some other credit institution without stating the recipient.

- The messages do not contain all the identification data of the ordering customer, e.g. one of our customers.

### ***2.6. Money laundering through foreign operations***

- Use of credit lines or other funding methods for foreign transfers when the transaction is not justified by the customer's usual activity.

- Establishment of large balances, that do not concord with the known movements of the customer's business, followed by subsequent transfers to foreign accounts.

- Transactions, that are not justified by the customer's activity, with branches of the financial institutions located in countries known for drug trafficking or as harbouring offshore entities.

- Significant transactions made by customers recommended by a financial institution from countries associated with the production, processing and sale of drugs.

- Foreign transfers from own foreign currency current accounts by residents whose normal activity does not justify the declared nature of the forex operation.

- Regular and important electronic foreign transfers made by individuals when the DPVE (foreign currency payment order) form is filled in according to the bona fide principle.

- Customer's failure to fulfil the obligation of transfer or repatriation in convertible currency and/or the national currency of all the amounts gained from operations with other countries.

- Significant forex operations made by resident customers (inexistence of incidental character).

- Foreign advance payments for imports, where commodities were not shipped, operation was not performed, the service was not provided within the contract term, not followed by the reimbursement of the advance, repatriation of amounts, justification of advance payments respectively.

- The payment of Foreign Currency Collection Statements (DIV) with cash amounts, paid by various persons instead of paying them by bank transfers.

- Repeated external transfers with the recommendation that the recipient receive the money in cash.

- External transfers made to other beneficiaries than the ones stipulated in Import Customs Declarations or in external invoices (redirected payments).

- Repeated external transfers to the third party, other than the external business partner of the client.

- External transfers representing „payments of import merchandise" to other legal or natural person than the merchandise provider.

- External transfers to companies registered in tax heavens, having the motivation „buying share company".

### ***2.7. Money laundering through loan operations***

- Customers that repay loans unexpectedly, very quickly, with funds from unknown sources.

- Loan purpose declared by customer is not justified and customer proposes cash collateral whose origin is unknown or mentions it when specifying loan purpose.

- Corporate customers apply for loans although an economic-financial analysis of their status does not evince the need for a loan.

- Use of loan proceeds in a manner that is inconsistent with the stated purpose of the loan.

- Customers that change the destination of the loan.

- Loan proceeds unexpectedly are wired or mailed to an offshore bank or third party.

- Loan applications accompanied by collateral from third parties or from a bank if the origin of that collateral is unknown or if it is not in conformity with the customer's status.

- Collateral put up by third parties that are not known to the bank, that do not have a close relationship with the customers and no plausible reason to put up with such security.

- Loan application accompanied by collateral consisting of a certificate of deposit issued by a foreign bank.

- Customer buys certificates of deposit, which he/she places as loan security.

- Requests for loans to offshore companies, or loans secured by obligations of offshore banks.

- Transactions involving an offshore “shell” bank whose name may be very similar to the name of a major legitimate institution.

- Incoming payments under the heading of “credit facility” or “loan” or “advance”, in particular, where payments are from abroad, the indicated lender being a letter-box company or an individual or an enterprise who/which has no relationship to the customer.

- Payments done with third party checks or with checks with multiple endorsements.

- Loan applications submitted by new customers through financial agents (lawyers, financial advisers, and brokerage companies).

- Promise of large hard currency deposits in consideration for favourable treatment on loan requests.

- Withdrawals from currency credit lines used, at exchange rate currency- ROL, for chain current payments with the same value, directed to different companies, the last company from the chain making external payments in advance, at exchange rate ROL-currency.

- Repayment of the loan by different company that the one which engaged the loan (it can be more suspicious if there is an off–shore company).

### ***2.8. Money laundering through investment related transactions***

- Purchase of securities kept safe by banks when this is not in accordance with the customer’s economic profile

- Requests by customers to have their investments managed (either in foreign currency or titles) when the sources of funds are not obvious or not in accordance with the customer’s economic profile.

- Purchase (trading) or sale of securities for cash to the end of purchasing other securities when the transaction is not made through the customer’s current account.

- Sale of unusually large amounts of securities into cash subsequently withdrawn.

- Use of cash for the purchase/sale of securities instead of non-cash settlements (transfers) particularly when it comes to substantial amounts.

- Request by a customer for the issuance by the bank of a safe keeping receipt for titles the authenticity of which cannot be verified.

- Maintenance of business of multiple accounts or investments for no apparent business purposes.

***2.9. Unusual circumstances/ features in documentary business and concerning guarantees***

- Use of letters of credit and other methods of international trade financing is such methods are not consistent with the usual business activities of the customer.

- The applicant or the beneficiary (drawer) indicated are unknown letter-box companies;

- The name of the beneficiary of the guarantee is not mentioned.

- LCs, documentary collections or guarantees concerning supplies of goods (in particular, raw materials) to countries, which usually do not have any demand for such goods or from countries which up till then did not appear as exporters of such products for lack of supplies.

- Indication that the guarantee is divisible, often including the addendum: transferable and divisible without payment of any transfer fee.

- Indication of non-existing ICC forms.

- Use of the term “Prime Bank Guarantee” or “PBG”.

- The customer submits unusual and incomplete documentation, or uses names very similar to those of major well-known lawful institutions, and/or uses ambiguous language or pseudo-expert terms, expressions and conditions, such as:
    - “maturity plus one day”;
    - “maturity 10 years plus one day”;
    - “fixed interest rate and market level/or better”;
    - “good, clean, clear and free funds”;
    - “closing off funding”;
    - “prime bank notes”;
    - “prime world bank guarantee”;
    - “top hundred bank promissory notes”;
    - “confirmation with fall-back responsibility”;
    - “no circumvention”, “no disclosure”;
    - “professional privacy and client confidentiality”;
    - “full legal corporate authority”;
    - “window time”.

# CHAPTER II
# ANOMALY INDICATORS
# FOR FINANCIAL INVESTMENT SERVICES COMPANIES

- Transactions for amounts that appear to be inconsistent to the customer's profile or known income-earning capacities, or business activity.
- Accounts opened with large cash deposits or frequent purchases, for amounts that are large or unjustifiably split up, of financial instruments paid for in cash.
- Trading in financial instruments where the transactions are not channelled through the customer's current account:
    - financial instruments presented for redemption in cash or for the purchase of other financial instruments, without going through the customer's current account;
    - partial or total disposal of financial instruments with the transfer of amounts to financial centres different from those specified in the contract, or in favour of persons other than those in whose names the instruments were registered, or to persons in whose names they have been jointly registered only in the last few months of the investment contract.
- Anomalous use of the trading accounts:
    - Buying and selling of a security with no discernible purpose, in circumstances which appear unusual and not linked to investment or risk diversification.
    - Transactions not in keeping with normal practice in the market in which they relate (e.g. with reference to market size and frequency or at off market prices, early termination of products at loss), especially where cash had been tendered/and or the refund checks is to a third party.
    - Trading in financial instruments not widely distributed among the public that is repeated at short intervals and/or involves large amounts, especially if with counterparts located in non-EU or non-OECD countries.
    - Use of the account only to carry out a limited number of transactions (usually followed by a substantial transfer of the funds into another account).
    - Dormant/inactive accounts that suddenly become active with large cash transactions.
    - Transfers of funds toward financial/banking institutions other than the one from which the original inflows have been channelled (especially if located in different countries).
    - The entry of matching buys and sells in particular securities ("wash trading") creating an illusion of trading. Such wash trading does not result in a bona fide market position and might provide cover for a money launderer. Wash trading through multiple accounts might be used to transfer funds between accounts by generating offsetting losses and profits in different accounts (see ex).

- Transfers of position between accounts that do not appear to be commonly controlled.

- Use of joint registration techniques for contracts involving financial instruments or changes in the names of the persons they are registered in for no apparent reason:
  - request for the splitting up of the investment into several transactions of the same kind registered jointly with different people that is not justified on grounds of risk spreading or portfolio diversification;
  - opening of several joint accounts or contracts on financial instruments by the same specific person with different other people;
  - unusually frequent changes of the names in which contracts involving financial instruments are registered or changes at the time the financial position is disinvested.

- Transactions involving Overseas Jurisdictions
  - a customer introduced by an overseas bank affiliate or other customer when both customer and introducer are based in countries known for drug trafficking.
  - A large number of security transactions across a number of jurisdictions.

- Transactions involving Unidentified Parties
  - A personal customer for whom clarification or identity proves unusually difficult and who is reluctant to provide details
  - A corporate /trust customer where there are difficulties and delays in obtaining copies of the accounts or other documents of incorporation.
  - Any transaction in which the counterparts to the transaction is unknown.
  - Incoming payments made with third party checks or checks with multiple endorsements.

- The customer has unusual concern about the financial intermediary's compliance with reporting requirements and the anti-money laundering policies;

- When the customer opens an account and he refuses to reveal information referring to his business activities;

- The customer is interested to pay higher charges to the financial intermediary to keep secret some information;

- One customer opens multiple accounts (for no apparent reason) in the name of family members or other persons;

- The customer can't provide relevant information related to the source of his funds;

- The customer has no sufficient information related to the nature of his activity;

- When the client opens an account, he exhibits a lack of concern regarding risks, commissions, other costs;

- The customer opens an account and he makes a fund deposit for purchasing a long-term instruments. After a very short period of time, the customer requests the liquidation of the position and the transfer of the funds in another account;

- The customer uses multiple foreign or domestic banks;

- The customer's transactions are extremely complex, but the customer's profile indicates a client with no experience in the securities field;

- The customer has accounts in a country identified as a non-cooperative territory by the FATF;

- The customer is engaged in cash transactions that seems to be structured to avoid the 10.000 EURO reporting requirement (ex. transaction with amount of 9.900 EURO);

- "Cross transaction" between/with off-shore companies or affiliated persons accounts;

- Trading confirmation or other document sent by the investment firm to the same address/person for apparently different accounts.

- Information provided by the client, in order to be identified the legitimate origin of his funds, is false, eronate or totally incorrect.

- The client (or other official associate) has a difuse background or is shown by mass–media as being related to possible infringments of the penal law.

- The client seems to act as agent on behalf of the orderer, whom identity is unknown, and declines, is reluctant or unclear, without having ground reasons, in providing information about that natural or legal person.

- The client performes transactions which have apparently no logic, do not follow a clear investments strategy or is not in concordance with the business strategy declared by the client.

- The client mixes "the bussiness goods" with his personal ones.

- The client requests that transaction to be processed in that way to avoid usual identification requirements.

Example 1

A company, established in an offshore centre, opens an account in an offshore bank (A) and subsequently opens another account in the financial institution (B) where the funds are then transferred. Only a very limited number of transactions are carried out in B before a substantial transfer is ordered towards another account opened in a name other than the holder of A and B in a "respectable" bank/financial institution (C). The purpose of the opening of the second account (B) is to provide the final holder funds that appear to have a legitimate origin, as well as to make the tracing of the funds' origins less transparent.

Example 2

Different individuals connected to each other open several accounts, for the purpose of trading between each other financial instruments over the counter, avoiding going through the market. At each transaction, the instrument is exchanged at a growing price. The various accounts are credited in cash or with transfers from foreign banks. Eventually, the account of the last seller is credited with a huge profit, while the account held by the last purchaser registers a big loss. A large transfer of funds is then ordered from the last seller's account to an account opened in another institution. The aim of the scheme is to provide a legitimate appearance to the funds credited in the latter institution.

# CHAPTER III

# ANOMALY INDICATORS FOR FINANCE COMPANIES

- A customer relationship with the finance company that does not appear to make economic sense. (e.g. a customer having a large number of accounts with the same finance company, frequent transfers between different accounts or exaggerated high liquidity).

- Customers that repay loans unexpectedly, very quickly, with funds from unknown sources.

- Loan purpose declared by customer is not justified and customer proposes cash collateral whose origin is unknown or mentions it when specifying loan purpose.

- Corporate customers apply for loans although an economic-financial analysis of their status does not evince the need for a loan.

- Customer buys certificates of deposit, which he/she places as loan security.

- Transaction in which assets are withdrawn immediately after been deposited unless the customer's business activities furnish a plausible reason for the immediate withdrawal.

- Loan proceeds unexpectedly are wired or mailed to an offshore bank or third party.

- Transactions that cannot be reconciled with the usual activities of the customer (e.g. use of letters of credit/other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.

- Use of loan proceeds in a manner that is inconsistent with the stated purpose of the loan.

- Customers that change the destination of the loan.

- Provision of personal guaranties or indemnities as collateral for loans between third parties that are not in conformity with market conditions.

- Back-to back loans without any identifiable and legally admissible purpose.

- Paying in large third party checks endorsed in favour of the customer.

- Loan applications accompanied by collateral from third parties or from a bank if the origin of that collateral is unknown or if it is not in conformity with the customer's status.

- Collateral put up by third parties that are not known to the bank, that do not have a close relationship with the customers and no plausible reason to put up with such security.

- Requests for loans to offshore companies, or loans secured by obligations of offshore banks.

- Transactions involving an offshore “shell” bank whose name may be very similar to the name of a major legitimate institution.

- Incoming payments under the heading of “credit facility” or “loan” or “advance”, in particular, where payments are from abroad, the indicated lender being a letter-box company or an individual or an enterprise who/which has no relationship to the customer.

- Loan applications submitted by new customers through financial agents (lawyers, financial advisers, and brokerage companies).

- Promise of large hard currency deposits in consideration for favourable treatment on loan requests.

# CHAPTER IV

# ANOMALY INDICATORS FOR INSURANCE COMPANIES

Money laundering poses a threat to insurance companies especially in regards to life insurance products or capitalization products. Special attention should be paid to the following cases**:**

- Purchase of life insurance policies that require the payment of high premiums and that appear to be inconsistent to the customer's economic profile or to his income-earning capacity. For example, customers known to be in financial difficulties, who sign high value policies
- Request to pay large premiums in cash
    - Frequent payments of the premiums in cash or foreign currencies for large amounts, which appear to be inconsistent to the customer's financial capacities or to his activity.
    - Frequent payments of the premiums in cash carried out for fractioned amount, where it appears that the purpose is to avoid the identification/reporting requirements.
- Signing of several insurance policies with payment of the premiums using third party checks, especially where there is no apparent connection between the third party and the customer, or checks with multiple endorsements.
- Use of joint registration techniques for contracts involving life insurance policies or changes in the names of the persons they are registered in for no apparent reason:
    - signing by the same contractor of several life insurance policies of the same kind with different beneficiaries.
    - recurrence of a particular name in which a number of contracts involving insurance policies are jointly registered together with different people's names;
    - unusually frequent changes in the names in which contracts involving insurance policies are registered or changes at the time the investment is liquidated;
    - Liquidation in a short span of time of benefits to the same person of a series of policies taken out by different customers.
    - Change in the name of the insured and/or the beneficiary of insurance policies in favour of third parties not belonging to the family of the insured or not linked to it in a way that would justify the change;
    - Naming of several beneficiaries for life insurance policies so that the amount to be paid to each of them is a fraction of a total sum which otherwise would be consistent with the identification/reporting requirement, in a manner that is not

justified by the relationships between the customer and the beneficiaries (e.g. family or business relations).

- Signing of several life insurance policies for which the beneficiary is the bearer of the policy.
- Customers who avoid direct contacts with the intermediary's employees or collaborators giving frequent mandates or proxies in a manner that appears unjustified.
- Transactions that are carried out providing untruthful or inexact essential information on purpose.
- Transactions involving foreign counterparts
  - Transactions that *involve transfers* towards foreign countries, that do not appear justified by the client's activity or other circumstances
  - Insurance policies signed by contractors that are residents in an off-shore centre or in areas known to be involved in drug trafficking, unless justified by business activity or other circumstances.
  - Overpayment of premium with a request to refund the excess to a third party or to a different country
- Capitalization schemes and life insurance contracts opened or managed in an anomalous way:
  - Payment of a capitalization scheme contract with the delivery of securities or other assets whose possession is not justified by the contractor's income-earning capacity and type of business
  - Large and/or simultaneous requests of advance redemption of policies and/or their use to obtain loans, especially where this involves accepting disadvantageous conditions, or frequent partial cashing in of large single-premium policies.
  - Request to exert the right to countermand the policy or to exercise the escape clause in the case of policies requiring a payment of large premiums.
  - Request at maturity to receive the payments in cash or with several checks for fractioned amounts.
  - Customers who sign policies or pay premiums to insurance brokers in areas that appear to be anomalous considering their own area of residence or of business activity.
  - Employees or agents who have very high activity levels of single premium business far in excess of any average company expectation.

Example no. 1

Contractor A signs a life insurance policy naming six different beneficiaries, so that at maturity, the payment to each beneficiary can be requested in cash (the fractioning is done with the purpose of avoiding the reporting requirements.

Example no. 2

A customer signs a one-premium life insurance policy for a significant amount (e.g. 100.000 Euro) with payment of the premium via a transfer originated from abroad (A). Though the maturity is indicated, for instance, in 10 years time, he/she nevertheless asks for advance redemption accepting the penalty clause, asking for the due to be paid with a check or through a transfer into a bank account (B) (the purpose of this transaction is to create a false appearance of legitimacy of the funds A)

Example no. 3

A loan is granted to a customer using a life insurance policy as collateral. The payment of the premiums is done periodically with dirty money and in a way that the reporting threshold is never reached (the anomaly in this case is both the use of cash instead of other traceable forms of payment and the amount which is always slightly below the reporting threshold).

# CHAPTER V
# ANOMALY INDICATORS FOR CASINOS

*(In certain instances, if the customers are properly identified by casinos, there may be facts and circumstances, which provides a reasonable explanation for the transaction that could remove it from the suspicious category.*)

- Customers structuring currency transaction at a casino:
  - Two or more customers purchase chips with currency (for amounts than are slightly lower than the reporting threshold) and then engage in minimal gambling. They subsequently combine all of their chips together and one of them goes to the cage to redeem the chips amounting in excess of the reporting threshold.
  - Customer asking a casino employee to monitor his/her gaming activity and to notify him when such activity is close to reaching the reporting threshold and, ounce notified, concludes gaming at that location, moves to another table and conducts additional cash transactions.
- Using others to structure cash transactions at casinos:
  - A customer, who is a big winner, enlists another customer to cash out some of the chips to avoid the reporting requirements.
  - A customer (other than a junket operator known by the casino to be engaged in the business of organizing gambling tours) is observed directly supplying large amounts of currency to individuals who then use the currency for the purchase of chips or exchange of currency.

- Customers engaging minimal activity without reasonable explanation:
  - A customer purchases a large amount of chips in cash at a table, engages in minimal gaming, and then goes to the cage to redeem the chips.

- Customers or junket operator providing false information/ identification.

- Customers unduly trying to bribe, influence, corrupt, or conspire with an employee for the purpose of avoiding reporting requirements (for example, by asking to structure the redemption payments, or recording the cash transaction in the name other individuals).

- Anomalous gambling activity, aimed at reducing gambling risks to the minimum:
  - A pair of bettors frequently cover between them both sides of an even bet (eg. Betting both red and black, or odd and even on roulette, or betting both with and against the bank in baccarat).
  - A customer purchases chips with cash, wagers with little chance of loss (e.g. bets both red and black on roulette) and conducts similar transactions and later goes to the cage to redeem the chips for large denomination bills.

- Buying chips with small-denominated notes, engaging minimal gaming or no gaming activity, and subsequently redeeming the (remaining) chips in cash, requesting high denominated notes.

# CHAPTER VI
# INDICATORS FOR LAWYERS, ACCOUNTANTS (AUDITORS) AND NOTARIES

Professionals must acquire an adequate knowledge of their clients by means of information concerning, in particular, the activities they conduct, as well as the economic profile and the aims of their work; they must continually evaluate their relations with their clients and ascertain any incongruence regarding their economic capacity, their activities conducted and their risk profile. In fact, the professional should keep in mind that dishonest clients may aim to use the professional's business standing in order to gain access to respectable known financial institutions, avoiding providing extensive information that would otherwise be requested by the financial institutions *(see the general part)*

To aid the detection of suspicious transactions they should consider the following factors:

a) the client's use of the professional for performing of financial or real estate transactions on his behalf, so as to avoid raising suspicion. In this case the client relies on the professional's credentials and reliability to avoid identification requirements;

b) the involvement of parties or subjects constituted, operating or established in countries with privileged regimes as regards their fiscal profile or their banking secrecy or in countries indicated by the Group of International Financial Action (GAFI) as non-cooperative;

c) operations planned or effected in conditions or with values clearly different from those of the market;

d) operations which appear incongruous regarding the aims declared;

e) the existence of unjustified incongruencies regarding the subjective characteristics of the client and his normal scope of operations, both in a quantitative sense, and in that of the contractual schemes utilized;

f) the unjustified recourse to techniques of splitting of the operations;

g) the unjustified interposition of third parties;

h) the unjustified use of ready cash or of inappropriate means of payment as regards the usual practice and considering the nature of the operation;

i) the behavior of the clients, taking account of the following factors, among others:

- ♦ reticence to supply complete information as regards their personal identity, the legal or administrative seat of their firm or company, the identity of the firm or company's representatives, those participating in the capital or any other subjects concerned, or the indication of data which is clearly false;

♦ reticence to supply complete information as regards the question or issue for which the intervention of the professional is required and the concrete aims and intentions of the client.

**Catalogue of anomaly indicators**

- Frequent operations of acquisition and cessation of firms, enterprises or companies, which are not justified by the nature of the activity conducted or the economic characteristics of the interested parties.

- Conferment or payments towards firms, enterprises or companies effected with modalities and entities, which may seem incoherent with the economic profile of the client or with the declared aims of the firms, enterprises or companies receiving the payments.

- Conferment or payments towards firms, enterprises or companies by means of third parties which are clearly extraneous to the operations required.

- Creation of corporate vehicles or other complex legal arrangements (holdings, for example) whose complexity and articulation, although in relation to the distribution of the shares and the foreign locations of one or more companies, seem to have the aim or intention of eluding, dissimulating or creating obstacles towards the identification of the provenance of the funds involved and those who have made them available.

- Creation of non-trading real estate investment companies, used to purchase real estates, who seem to have the aim of dissimulating the origin of funds involved.

- Conferment of promotions and positions of responsibility in firms, enterprises or companies to persons clearly not in possession of the necessary capacities and which are clearly intended to separate decision making activities from those people officially in management positions.

- Accounting operations intended to conceal or hide, for example by means of the over-evaluation or the under-evaluation of goods, sources of income of various nature or provenience.

- Requests for financial and tax advice. Criminals with a large amount of money to invest may present themselves as individuals wishing to reduce their tax liabilities or desiring to place assets out of reach in order to avoid future liabilities

- Searching for funding or financing on the basis of guarantees, also represented by assets or certificates, which attest to the existence of deposits in foreign banks, especially if these deposits are held in foreign banks residing in those countries indicated by the GAFI as non-cooperative or characterized by a privileged fiscal regime, in the absence of adequate justificatory reasons.

# CHAPTER VII
# INDICATORS FOR EXCHANGE HOUSES

- Repeated requests for the exchange of currency for amounts that slightly less than the reporting limit in a short period of time, also through several different branches.

- Purchase or sale of large quantity of currencies, or the exchange of foreign currency for a different foreign currency.

- Exchanging an unusually large amount of small-denominated notes for those of higher denomination.

- Client´s refusal to be identified when he requires performing currency exchange transaction.

# CHAPTER VIII

# INDICATORS FOR THE ENTITIES OPERATING MONEY TRANSFER SERVICES (Post Offices, Banks, Money Transfers)

- Transfers ordered by the customer payable to himself or to the same individual in several countries in a short period of time without any reasonable explanation.

- Repeated transactions of the same kind not justified by the customer's activity that seem to be carried out for the purpose of dissimulation:
  - frequent inflows of funds that are transferred after a short interval in ways or to destinations unrelated to the customer's normal activity, especially if the origin or destination is abroad;
  - inflows in the form of instruments (cash, credit instruments, credit transfers) that do not appear consistent with the customer's activity.

- Recourse to repeated transactions for small amounts that appear to be aimed at avoiding identification and reporting requirements (e.g.: frequent transactions for amounts just below the reporting threshold, especially if in cash or carried out through several different subsidiaries of the same R.E., where this is not justified by the customer's activity);

- Large transactions, which appear to be unusual, compared to the client's previous transactions, or for which there appears to be no plausible economic or financial reasons (e.g.: large transactions made in the name of the company by directors or persons related to them drawing on resources unrelated to the activity of the company, especially if in cash).

- Transactions set up in a way that is illogical, especially if they are economically or financially disadvantageous for the customer.

- Transactions carried out frequently by a customer in the name of or in favour of third parties, where such dealings do not appear justified.

- Transactions carried out by clients who, without a plausible reason, frequently use one or more offices of money remittance services far from their residence or far from the area of their activity.

- Transactions carried out by third parties in the name of or in favour of a customer for no plausible reason.

- Transactions requested with obviously inexact or incomplete details, suggesting the intention of hiding essential information, especially if this concerns parties interested in the transaction.

- Transactions involving counter-parties located in offshore centres or geographical areas well known for drug trafficking that are not justified by the economic activity of the customer or other circumstances.

# CHAPTER IX

# INDICATORS FOR THE REMAINING REPORTING ENTITIES
# (Real Estate Agencies, Auctioneers)

- High-value transactions, which do not appear coherent with the client's economic profile.

- Requests by clients or by their representatives to settle high-value transaction with the unjustified use of ready cash or of inappropriate means of payment as regards to the usual practice and considering the nature of the operation.

- Representatives, who are reluctant to indicate the subjects they are acting for, renounce to conclude the transaction when asked to give documented information about their clients or indicate as final buyer a subject different from the one indicated before.

- Purchase of high-value goods, sold again after a short period of time, even at a lower price.

- High-value transaction performed by (or in the interest of) natural or legal persons with seat in countries known as harboring illegal or offshore activities.

# ANNEX

## THE LEGISLATION
## ON ANTI-MONEY LAUNDERING

# THE PARLIAMENT OF ROMANIA

## LAW no. 656/07.12.2002

### on the Prevention and Sanctioning of Money Laundering
### The Parliament of Romania adopts this law

### Chapter I
### General Provisions

**Art. 1** – This Law establishes measures on the prevention and combating of money laundering.

**Art. 2** – For the purpose of this Law:

a) "money laundering" means the offence provided for in art. 23;
b) "property" means the assets of every kind, whether corporeal or incorporeal, movable or immovable, as well as legal documents or instruments attesting a title or a right in respect to such assets;
**c)** "suspicious transaction" means any transaction, which by its nature and unusual character, compared to the activities of the client, raises suspicions of money laundering.

### CHAPTER II
### Customer identification and data processing procedures regarding money laundering information

**Art. - 3**

**(1)** As soon as an employee of a legal or a natural person of those stipulated in article 8, has suspicions that a transaction, which is on the way to be performed, has the purpose of money laundering, he shall inform the person appointed according to art. 14, para (1), who shall notify immediately the National Office for Prevention and Control of Money Laundering, hereinafter referred to as "the Office". The Office shall confirm the receipt of the notification.

**(2)** If the Office considers as necessary, it may decide to suspend the transaction for 48 hours, based on the existing reasons.

**(3)** Before this deadline, if the Office considers that 48 hours are not enough, it may request to the General Prosecutor's Office by the Supreme Court of Justice to extend the suspension for maximum 3 working days, based on the existing reasons. The General Prosecutor's Office by the Supreme Court of Justice may authorise only once the requested extension or may order the cessation of the transaction's suspension.

**(4)** Within 24 hours, the Office must notify the persons provided in art. 8, the decision to suspend the transaction or the disposition to extend the period of suspension, authorised by the General Prosecutor's Office by the Supreme Court of Justice.

**(5)** If the Office didn't make the notification, within the period provided in para (4), the persons referred to in art. 8, may carry out the transaction.
**(6)** The persons provided in article 8 or the persons designated in accordance with art. 14 para (1) shall report to the Office, within 24 hours, about all cash transactions performed, in ROL or in foreign currency, whose minimum limit represents the equivalent of Euro 10,000, irrespective whether the transaction is carried out in a single operation or in several linked operations.
**(7)** The provisions under paragraph (6) shall also apply to cross-border transfers to/from accounts, for amounts exceeding the equivalent of Euro 10,000.
**(8)** The following categories of operations, carried out by the State Treasury, are excepted from the obligation to be reported to the Office: cash amounts for salary payments, payments made by public institutions, collection of taxes, contributions and any other budgetary obligations from natural and legal persons, including cash amounts deposited by public institutions, as well as the operations provided in para (7).
**(9)** The Board of the Office shall decide on the reporting form to be used for the operations provided in paragraphs (1), (6) and (7), within 30 days from the entering into force of this Law.

**Art. - 4**
If the persons provided in article 8 have knowledge that a transaction, for which they have received instructions to perform it, has the purpose of money laundering, they may perform the transaction without a prior notification to the Office, if the transaction must be carried out immediately or, if by not performing it, the efforts to trace the beneficiaries of such money laundering suspect operation could be hampered. These persons have the obligation to notify the Office immediately, but not later than 24 hours, about the performed transaction, specifying the reason for non-compliance to the provisions of art. 3.

**Art. - 5**
**(1)** The Office may require to the persons referred to in art.8, as well as to the competent institutions, data and information necessary to perform its competences provided by the Law. The information related to the notifications received according to the art. 3 and 4 is subject to confidentiality.
**(2)** The persons provided in art. 8 shall submit to the Office the required data and information, within 30 days, from the date of receiving the request.
**(3)** The professional secrecy related to the entities mentioned in article 8 is not opposable to the Office.
**(4)** The Office may exchange information, based on reciprocity, with foreign institutions having similar functions and which are equally obliged to secrecy, if such information exchange is made with the purpose of preventing and combating money laundering.

**Art. - 6**
**(1)** The Office shall analyse and process the information received, and if there are serious grounds of money laundering, the information shall be immediately submitted to the General Prosecutor's Office by the Supreme Court of Justice.

**(2)** If, after analysing and processing the information received, serious grounds for money laundering are not found, the Office shall keep the information in its own database.
**(3)** If the information provided for in para (2) are not completed within 5 years, they are filed within the Office.
**(4)** After receiving the information, the General Prosecutor's Office by the Supreme Court of Justice may request additional information to the Office, if it appreciates that the information is not sufficient.
**(5)** The Office has the obligation to transmit to the General Prosecutor's Office by the Supreme Court of Justice, or as appropriate, to the National Anti-Corruption Prosecutor's Office, on their request, data and information obtained according to the provisions of this Law.
**(6)** The General Prosecutor's Office by the Supreme Court of Justice informs the Office, quarterly, on its request, about the stage of legal proceedings in the cases received from the Office.

**Art. - 7**
Information supplied in good faith, in accordance with the provisions of the art. 3-5, by the persons provided in article 8 or by the persons appointed in accordance with art. 14 para (1) may not result in disciplinary, civil or penal liability of these persons.

**Art. - 8**
The provisions of this Law shall be applied to:
a) banks, foreign banks branches and credit institutions;
b) financial institutions, such as: investment funds, investment companies, investment administration companies, depositary companies, custody companies, securities companies, pension funds and other such funds, which perform the following operations: crediting, including inter alia, consumption credit, mortgage credit, factoring, financing of commercial transactions, including forfeiting, financial leasing, payment operations, issuing and administration of payment means, credit cards, travelers cheques and other alike, granting or undertaking of guarantees and underwriting of commitments, transactions on own account or on the clients account using the money market's instruments, cheques, payment orders, deposit certificates, etc., foreign exchange, derivatives, financial instruments related to foreign exchange rates or interest rates, securities, participation to the issuance of shares and services related to the issuance, consultancy on capital structure for enterprises, industrial strategy, consultancy and services in the field of mergers and acquisitions of enterprises, brokerage on inter-banking market, portfolio administration and consultancy on portfolio administration, custody and administration of securities;
c) insurance and reinsurance companies;
d) economic agents performing gambling and pawning activities, trading in works of art, precious metals and stones, dealers, tourism operators, services providers and any other similar activities involving movement of values;
e) natural and legal persons providing legal, notarial, accounting, financial and banking advice, notwithstanding their professional secrecy legal provisions;
f) persons with attributions in the privatisation process;
g) post offices and legal persons who provide money transmission/remittance services in ROL or foreign currency;

h) real estate agents;
i) state treasury;
j) foreign exchange offices (« bureaux de change »);
k) any other natural or legal person, for acts and deeds committed outside the financial and banking system.

**Art. - 9**
**(1)** The persons provided in article 8 have the obligation to establish the identity of their customers, when entering into business relations, opening accounts or offering services.
**(2)** The identification requirement applies also to any transactions, other than those provided in the paragraph 1, whose minimum value is equivalent to EUR 10,000, irrespective whether the transaction is carried out in a single operation or in several linked operations.
**(3)** As soon as there is any information that the transaction has the purpose of money laundering, the customers' identification shall be made, even if the value of the transaction is lower than the minimum limit provided in para (2).
**(4)** Where the sum is not known at the time when the transaction is accepted, the natural or legal person having the obligation to identify the customers, shall immediately proceed with their identification, as soon as it knows the value of the transaction and when it has been established that the minimum limit provided in para (2) has been reached.
**(5)** The provisions of para 1-4 shall apply also to all transactions involving persons who are not physically present for identification purposes (non - face - to - face operations).

**Art. - 10**
**(1)** Identification data regarding customers shall include:
a) for natural persons: data mentioned in the identity documents provided by the law;
b) for legal persons: data mentioned in the incorporation documents provided by the law, as well as the proof that the natural person performing the transaction is the legal representative of the legal person.
**(2)** for foreign legal persons, when opening bank accounts, there shall be requested those documents indicating the identity of the company, the address, the type of company, the place of incorporation, the special power of attorney for the person representing the company in the transaction, as well as a translation in Romanian of the respective documents, certified by a public notary.

**Art. - 11**

In cases where there are information referring to the customers provided in art. 9 and 10, that the transaction is not performed in their own name, the legal persons mentioned in art. 8 shall take measures in order to obtain information about the real identity of the person on whose interest or behalf are acting these customers, including information from the Office.

**Art. - 12**
**(1)** Identification requirements shall not apply to insurance and reinsurance companies provided in article 8, concerning life insurance policies, if the insurance premium or the annual rates are lower or equal to the equivalent in

ROL of EUR 1,000 or if the single insurance premium paid does not exceed the equivalent in ROL of EUR 2,500. If the periodical premium rates or the amounts to be paid in any given year are higher or will be increased so as to exceed the EUR 1,000 threshold or respectively EUR 2,500 equivalent in ROL, the identification of the customers shall be required.
**(2)** Identification requirements shall not be compulsory for the subscription of insurance policies issued by the pension funds, obtained by virtue of a labour contract or due to the profession of the insured person, on condition that such policy may not be redeemed before maturity and may not be used as a guarantee or collateral in order to obtain a loan.
**(3)** Identification requirements shall not apply when it has been established that the payment shall be made by debiting an account opened on behalf of the client with a bank or a saving institution.

**Art. - 13**

**(1)** In each case when the identity is required according to the provisions of this Law, the legal or natural person provided in article 8, which has the obligation to identify the customer, shall keep a copy of the document, as identity proof or identity references, for a period of 5 years, from the date when the relationship with the customer ends.
**(2)** The persons referred to in art. 8 shall keep the secondary or operative records and the records of all financial transactions subject to this law, for a period of 5 years from the performance of every transaction, in an appropriate form, in order to be used as evidence in Court.

**Art. - 14**

**(1)** The legal persons provided in art. 8 shall appoint one or more persons having responsibilities in the enforcement of this law, whose names shall be notified to the Office, together with the nature and limits of the mentioned responsibilities.
**(2)** The persons appointed according to the paragraph 1 shall be responsible for the performance of the tasks established for the enforcement of this law.

**Art. - 15**

The persons designated according to the art. 14 paragraph (1) and the persons provided in art. 8 shall draw up a written report for each suspicious transaction, in the form established by the Office, which shall be immediately submitted to the Office.

**Art. - 16**

**(1)** The legal persons provided in art. 8 shall establish adequate procedures and methods of internal control, in order to prevent and combat money laundering, and shall ensure the training of their employees on detecting the transactions that could be related to money laundering and on taking the immediate measures in such situations.
**(2)** The Office shall participate to the special training programmes for the representatives of the persons provided in art.8.

**Art. - 17**

**(1)** The authorities with financial control powers, according to the law, and those with prudential supervision tasks on the persons referred to in art.8, shall verify and control the enforcement of the present law, within the performance of their legal duties, and if there are suspicions of money laundering or infringements to the provisions of the this law, they shall immediately notify the Office.

**(2)** The Office may perform joint checks and controls on the persons provided in art. 8, together with the authorities mentioned in para (1).

**Art. - 18**

**(1)** The personnel of the Office is obliged not to disclose any information received during its activity, except under legal conditions. This obligation remains valid for a period of 5 years after the end of the labour contract with the Office.

**(2)** The persons provided in art. 8 and their employees are obliged not to disclose the information they are holding, related to money laundering, except under legal conditions, and may not warn their customers regarding the notification to the Office.

**(3)** The use for personal purposes of the information received by the Office's personnel and by the employees of the persons provided in art. 8, during the activity and after its ceasing, is forbidden.

## CHAPTER III
## The National Office for the Prevention and Control of Money Laundering

**Art. - 19**

**(1)** The National Office for the Prevention and Control of Money Laundering is established as a specialized body and legal entity subordinated to the Government of Romania, having the premises in Bucharest.

**(2)** The activity object of the Office is the prevention and combating of money laundering, for which purpose it shall collect, analyse, process and submit information to the General Prosecutor's Office by the Supreme Court of Justice, according to the art.6 paragraph (1).

**(3)** In order to exercise its competences, the Office shall establish its own structure at central level, whose organization chart is approved through Government's Decision.

**(4)** The Office is managed by a President, ranking as Secretary of State, appointed by the Government, from among the Members of the Board of the Office, who shall also act as main credit ordinator.

**(5)** The Board of the Office is the debating and decisional structure, including one representative from each of the following institutions: the Ministry of Public Finances, the Ministry of Justice, the Ministry of Interior, the General Prosecutor's Office by the Supreme Court of Justice, the National Bank of Romania, the Court of Accounts and the Romanian Banking Association, appointed for a period of 5 years, through a Governmental Decision.

**(6)** Within the exercise of its attributions, the Board of the Office adopts decisions with a majority of votes.

**(7)** At the time of their appointment, the members of the Board shall fulfil the following requirements:

a) to hold an university degree and to have at least 10 years of experience in a legal or economic position;
b) to be domiciled in Romania;
c) to have Romanian citizenship only;
d) to be legally able to exercise civil and political rights;
e) to have a high professional and an intact moral reputation.
**(8)** It is forbidden for the members of the Board to be a member of a political party or to be involved in public activities with political character;
**(9)** The position as Member of the Board is incompatible with any other public or private position, except for didactic positions in the high education institutions.
**(10)** The Members of the Board have the obligation to immediately notify the President of the Office, in writing, should any situation of incompatibility occur.
**(11)** During the term of their mandate, the Members of the Board shall be seconded to the Office and their labor contracts with the institutions of origin shall be suspended. At the end of their mandate, they shall return to their initial position.
**(12)** If a position in the Board is vacant, the management of the competent authority shall propose to the Government another person, within 30 days from the date when the position has become vacant.
**(13)** The mandate of a Member of the Board shall cease in the following conditions:
a) at the expiration of the period for which he has been appointed;
b) by resignation;
c) by death;
d) by not being able to exercise the mandate for a period of more than 6 months;
e) upon occurrence of any incompatibility;
f) by revocation by the authority that appointed him.
**(14)** The employees of the Office may not hold any position or fulfill any other function in any of the institutions provided in article 8, while working for the Office.
**(15)** For the functioning of the Office, the Government shall transfer in its administration the necessary real estates – land and buildings – belonging to the public or private domain, within 60 days from the registration date of the application.
**(16)** The Office may participate to the activities organized by the international organizations in the field and may be member of these organizations. The Board of the Office decides on the opportunity to participate to such activities.

**Art. 20**
**(1)** The members of the Board shall benefit of the rights provided by the law for persons that hold positions of public dignity. The indemnity for the Board's Members shall be established according to the provision of art.19 and para 6 of the annex II/2 of the Law no. 154/1998 on wage system in the budgetary sector and indemnities for persons having a public dignity position, as modified and amended subsequently.
**(2)** The wage system for the specialised personnel and auxiliary specialised personnel shall apply in accordance with the Law no. 50/1996 on the wage system and other rights of the personnel of the judicial authority bodies, republished, as modified and amended subsequently.

**(3)** The classification of job positions, studies and years of experience requirements needed for the employment, promotion and level of wages of the Office's personnel, as well as the legal rules establishing the wage system are included in the Annex, which is part of this Law.
**(4)** The promotion of the Office's personnel on professional ranking and levels provided in para (2) shall be made using professional tests, in accordance with the years of experience requirements provided in the Annex to this Law.
**(5)** The basic indemnity for specialized personnel, as it has been established in Chapter I of the Annex of this Law is the unique form of monthly remuneration for the activity corresponding to the position held, without receiving any of the additional benefits provided by the Law no. 50/1996 on wages and other rights of the personnel from the judicial authority bodies, as modified and amended subsequently, and represents the basis for calculation of the rights and obligations determined in relation with the wage revenues.
**(6)** The auxiliary specialized personnel shall receive the additional benefits provided by the Law no. 50/1996, republished, as amended and completed by the Governmental Ordinance no. 83/2000, approved with amendments by the Law no. 334/2001, for the assimilated positions, beside the basic salary provided in the Annex to this Law.
**(7)** The personnel of the Office holding specifically positions for the budgetary system will be paid in accordance with the legislation referring to the personnel working in the ministries and other specialized central bodies.
**(8)** The employed personnel, having wages according to this law, has the right to receive, for the annual holiday period, beside the holiday indemnity, a premium equal to the gross basic indemnity or, as appropriate, the gross basic salary of the previous month before leaving on holiday, which is taxed separately.

## CHAPTER IV
## Responsibilities and penalties

**Art. - 21**
Violation of the provisions of this Law shall be subjected, as appropriate, to civil, disciplinary, contraventional or criminal liability.

**Art. - 22**
**(1)** Shall be considered as contravention the following deeds:
(a) Violation of the obligations of art. 3 para (1) and (6), art. 4 and art. 9;
(b) Violation of the obligations provided in art. 5 para (2), art. 11, art. 13-15, art. 16 para (1) and art. 17.
**(2)** The contraventions provided in para (1) a) shall be sanctioned by a fine ranging from 20,000,000 ROL to 100,000,000 ROL, and the contraventions provided in para (1) b) shall be sanctioned by a fine ranging from 30.000.000 ROL to 200.000.000 ROL.
**(3)** The sanctions provided in paragraph (2) shall be applicable also to legal entities.
**(4)** The contraventions shall be ascertained and fines shall be applied by the persons designated by the Office and by the authorities provided in article 17.
**(5)** The provisions of this Law referring to contraventions, shall be completed adequately with the provisions of the Governmental Ordinance no. 2/2001 on the legal regime of contraventions, approved with amendments and additional

provisions by the Law no. 180/2002, as subsequently modified, except for the art.28 and 29.

**Art. - 23**

**(1)** The following shall be considered as offence of money laundering and shall be punished with 3 to 12 years imprisonment:
a) the conversion or transfer of property, knowing that such property is derived from criminal activity, for the purpose of concealing or disguising the illicit origin of property or of assisting any person who is involved in the commission of such activity to evade the prosecution, trial and punishment execution;
b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from criminal activity;
c) the acquisition, possession or use of property, knowing, that such property is derived from criminal activity;
**(2)** Association to commit or initiation of an association, adhesion, or abetting in any kind of such an association for the purpose of committing the money laundering offence, shall be punished with 5 to 15 years of imprisonment.
**(3)** The attempt shall be punished.

**Art. - 24** Violations of the obligations provided in art.18 shall be considered as offence and shall be punished with 2 to 7 years of imprisonment.

**Art. - 25**
**(1)** For the offences provided in art. 23 and 24, shall be also applied the provisions of the art.118 of the Criminal Code on the confiscation of proceeds of crime.
**(2)** If the proceeds of crimes covered in art.23 are not found, their equivalent in money or the property acquired shall be confiscated instead of these proceeds.
**(3**) In order to guarantee the enforcement of confiscation of proceeds, the provisional measures provided in the Criminal Procedure Code shall be applied.

**Art. - 26**
For the offences provided in art.23 and 24, the banking and professional secrecy cannot be opposed to prosecution bodies, after the beginning of the penal procedures ordered by the prosecutor, nor to Courts. The data and information required by the prosecutor or by the Court shall be sent by the persons provided in art.8, on the prosecutor's written request, during the prosecution or on Court's request, during the trial.

**Art. - 27**
**(1)** If there are serious grounds that a person is going to commit a money laundering offence using telecommunication or IT systems, the prosecutor may order, for a certain period of time, the access to these systems.
**(2)** The prosecutor may also order, when there are serious grounds on committing the money laundering offence, the monitoring of the bank accounts and of the accounts assimilated to these, for a certain period of time.

**(3)** The provisions of art.$91^1$-$91^5$ of the Criminal Procedure Code shall apply accordingly.

## CHAPTER V

## Final Provisions

**Art. - 28**

The identification of customers, in accordance with art.9, shall be made starting with the date of entering into force of this Law.

**Art. - 29**

The minimum limit for the transactions provided in art. 9 para (2) and the maximum limit for the amounts provided in art. 12 para (1) may be changed by the Government's Decision, at the Office's proposal.

**Art. - 30**

Within 30 days from the entering into force of this Law, the Office shall submit to the Government for its approval, the new Regulations on Organisation and Functioning of the National Office for Prevention and Control of Money Laundering.

**Art. - 31**

The Law no. 21/1999 on the prevention and sanctioning of money laundering, published in the Official Gazette of Romania, Part I, no. 18 on 21 January 1999, as amended subsequently, shall be abrogated.

Bucharest, December 7, 2002
No. 656

# GOVERNMENT OF ROMANIA

## DECISION no. 479/16.05.2004
### for the Approval of the Regulation on the Organisation and Functioning of the National Office for the Prevention and Control of Money Laundering

Based on the provision stipulated in the art. 107 of the Romania's Constitution and of the Law no. 21/ 1999 on the Prevention and Sanctioning of Money Laundering, as amended subsequently,
The Government of Romania decides:

**Art. 1** - To approve the Regulation on the Organisation and Functioning of the National Office for the Prevention and Control of Money Laundering, provided for in the annex, which is entirely part of the present decision.
**Art. 2** – The security of the headquarters of the National Office for the Prevention and Control of Money Laundering and the entrance control is assured permanently and free of charge by the National Gendarmerie.
**Art. 3** – On the coming into force date of the present decision is repealed the Government Decision no. 413/1999 on the approval of the Regulation on the Organisation and Functioning of the National Office for the Prevention and Control of Money Laundering and its territorial structures, published in the Official Gazette of Romania, Part I, no. 249/02.06.1999.

PRIME - MINISTER
ADRIAN NASTASE

Countersigned by:
President of the National Office for the Prevention and Control of Money Laundering
Ioan Melinescu
Secretary of State
On behalf of the Minister of Public Finances
Gheorghe Gherghina
Secretary of State
Marian Sarbu
Minister of Labour and Social Solidarity

Bucharest, 16 May 2002
No. 479

**ANNEX**

# Regulations
# on the Organisation and Functioning of the National Office for the Prevention and Control of Money Laundering

## CHAPTER I
## General Provisions

**ART.1** (1) The National Office for the Prevention and Control of Money Laundering, hereinafter referred to as *"the Office"*, established according to the Law no. 21/1999 on the Prevention and Control of Money Laundering, as amended subsequently, hereinafter referred to as *"the Law",* is organized and operates as a specialized body having legal personality, subordinated to the Government.

(2) The headquarters of the Office is located in the town Bucharest, 202A, Splaiul Independentei, 8th floor, sector 6.

**Art.2** - The Office has, as activity object, the prevention and combating money laundering, in which purposes it receives, analyses and processes information and informs the authorities having competences granted by the law.

**Art.3** (1) The Office is managed by a President, ranking as Secretary of State, appointed by the Government, from among the Office's members. The President of the Office has also the quality of main credit ordinator.

(2) The Office Board includes a representative of each of the following institutions: the Ministry of Public Finances, the Ministry of Justice, the Ministry of Interior, the General Prosecutor's Office by the Supreme Court of Justice, the National Bank of Romania, the Romanian Bank's Association and Court of Accounts, appointed for a period of 5 years, through a Decision of the Government. The Office's Members hold public dignitary positions.

(3) The Office's Board set up in accordance with the art. 19 para (6) of the Law no. 21/1999, as amended subsequently, is the debating and decisional structure of the Office.

(4) The Office's staff is composed of specialty, auxiliary specialty personnel and personnel holding similar positions to those in the budgetary field and is formed of financial analysts, assistants to financial analysts, civil servants and contractual personnel.

(5) The maximum number of staff is 84.

(6) The Office sets up its own organization at the central level.

**Art.4** (1) The organizational chart is provided for in the annex, which is entirely part of the present Regulation.

(2) In accordance with the above-mentioned chart, through Board Decision, divisions, bureaus and departments could be organized.

## CHAPTER II
## Office's Attributions

**Art.5** In order to accomplish its activity object, the Office has the following main attributions:

a) receives data and information from the natural and legal entities provided for in the art.8 and 17 of Law no.21/1999, as amended subsequently concerning the operations and transactions performed in ROL and/or foreign currency;
b) analyses and processes the data and information received;
c) examines, on its own initiative, the cases within its area of competences;
d) requests from any competent body to provide data and information necessary to perform its activity object;
e) co-operates with the Ministry of Public Finances, the Ministry of Justice, the General Prosecutor's Office by the Supreme Court of Justice, the Ministry of Interior, the Romanian Intelligence Service, the Foreign Intelligence Service, the National Bank of Romania, the Court of Accounts, the Romanian Banks' Association, the National Securities Commission, the Insurance Supervisory Commission, Trade and Industry Chamber of Romania and Bucharest;
f) co-operates and promotes the exchange of information and experience with foreign entities having similar competences and with European Regional and International institutions with tasks in the field of combating money laundering;
g) issues, according to the law, decisions regarding the suspension of the performance of transaction, upon which is a suspicion related to money laundering;
h) informs the General Prosecutor's Office by the Supreme Court of Justice in the situations stipulated by the law;
i) draws up and brings up-to-date the lists including the natural and legal persons suspected of committing or financing terrorist acts, which are submitted to the Ministry of Public Finances in accordance with the provisions of the Emergency Government Ordinance no. 159/2001 on the prevention and combating the use of the financial-banking system for the purpose of financing terrorist acts;
j) ascertains the infringements committed in its activity field and imposes sanctions stipulated by the law, through the persons specially designated for this purpose;
k) observes the unitary application of the legal dispositions within its field of activity, by issuing decisions;
l) monitors the real application of its own decisions;
m) submits proposals to the Government and the central public administration bodies regarding the approval of measures related to the prevention and combating of money laundering, endorses draft of norms related to its activity field;
n) organizes specialized training programs for the natural persons and the representatives of the legal entities provided for in the art.8 of Law no. 21/1999, as amended subsequently, as well as of its own personnel;
o) draws up annual activity report or, whenever the Government decides, and performs surveys, analysis and syntheses related to its activity field;
p) establishes the form of written reports for transactions which could be related to the money laundering;

q) draws up, negotiates and concludes conventions, protocols agreements with similar institutions from other countries, in the limit of its mandate, given by the Government;

## CHAPTER III
## Organization and functioning of the Office

**Art.6** The organization, the structure and the functioning procedures of the Office have to assure the accomplishment of its attributions stipulated by the law and the present Regulation.

**Art.7** (1) The President represents the Office in the relations with the legislative, judicial, and administrative authorities, as well as, with natural and legal persons inside the country and abroad, including the international organizations and bodies.

(2) The President represents the Office as legal entity and through his signature commits, the patrimony of the institution in relation to the third parties.

(3) The President of the Office leads the Board meetings and controls the application of the adopted decisions, disposing the necessary measures.

(4) The President of the Office could delegate the powers of representation to other members of the Office's Board.

(5) The President issues employment orders and orders of cessation of activity, approves transfers and applies disciplinary sanctions stipulated by the law for the staff of the Office.

**Art.8** (1) The meetings of the Office's Board are hold in the presence of at least 4 members. The decisions of the Office's Board are adopted with majority of votes of the present members.

(2) The Board members ensure and co-operate with the institutions whose representatives they are.

(3) The Board debates and, as appropriate, decides over:

a) the suspicious transactions reports, including possible objections regarding to them, and decides on the measures to be taken;
b) the suspension of transaction for 24 hours and decides on formulation of the request to extend the suspension, addressed to the General Prosecutor's Office by the Supreme Court of Justice;
c) the information to be sent to the General Prosecutor's Office by the Supreme Court of Justice in cases in which there are facts and solid grounds related to money laundering;
d) lists including the persons suspected of committing terrorist acts or financing terrorist organizations;
e) points of view, recommendations and advices regarding the application of the legal provision in the field;
f) categories of agreements, association decisions and unified procedures proposed for endorsement;
g) draft of regulations to be submitted for the approval of the competent institutions.
h) activity report;
i) draft on own budget of revenues and expenditures;

j) drafting up, adoption and updating of the strategies and programs on prevention and combating money laundering;
k) establishment of the criteria for recruitment, promotion and professional training of the personnel;
l) elaboration and updating of the co-operation means with the internal authorities, in order to accomplish the Office's activity object;
m) establishment of the general guidelines for the co-operation with foreign authorities and international organizations and bodies, in order to harmonize related legislation;
n) allocation of attributions in the Office's area of competence to each of its members;
o) measures regarding the material and disciplinary responsibility of the hired personnel;

**Art.9** (1) Within the Office operates the following specialized directions:
a) Computer Technology, Synthesis and Operative Records Directorate;
b) Operative Directorate – analysis I;
c) Operative Directorate – analysis II;
d) Co-operation and International Relations Directorate;
e) Economic - Administrative Directorate;

(2) The Internal Audit Department and the Legal Bureau are functioning under the direct subordination of the President of the Office.

**Art.10** (1) The Computer Technology, Synthesis and Operative Records Directorate has the following main attributions:
a) draws up studies in view to acquire knowledge on the structure of the entities and the functioning environment in the activity area of the Office, general trends of the money laundering phenomenon, the effects of the money laundering phenomenon on financial-banking sector, the evolution of the phenomenon with the purposes to identify the situations in which taking subsequent measures is justified;
b) proposes to the Office Board the form of the reports, which are used in the reporting and notification process.
c) organizes the centralized records and administration of the Office's databases;
d) organizes centralized recording and management of the Office data base;
e) organizes the activities of registration, secretariat, secret documents bureau and archives;
f) elaborates analysis and synthesis materials in the field of activity of the Office;
g) realizes the specific record kipping of the natural and legal persons provided for in the art. 8 of the Law no. 21/1999, as amended subsequently;
h) receives, analyses and processes the suspicious transactions reports and reports on cash withdrawals and deposits, sent by the natural and legal persons stipulated in the art. 8 and 17 of the Law no. 21/1999, as amended subsequently;
i) proposes to Office's Board the analysis of the cases in which there are suspicions related to money laundering.

(2) The Operative Directorates perform the following main attributions:
a) receive, analyze and process the cases suspected of money laundering approved by the Office's Board;

b) request, according to the art.5 of the Law no. 21/1999,as amended subsequently, to any competent institution the information, necessary in the verification process of the cases suspected of money laundering;
c) draw up notes on the result of the verifications and submit them to the Office's Board debate.
d) ascertain the contravention and apply those sanctions stipulated in the art. 22 of the Law no. 21/1999, as amended subsequently, through the persons designated by Board.
e) Based on the Board decision, submit immediately to the General Prosecutor's Office by the Supreme Court of Justice the cases where there are solid grounds related to money laundering.

(3) Co-operation and International Relation Directorate has the following main attributions:

a) ensures the relations and co-operation on experience and information exchange with similar foreign institutions, with other specialized international bodies.
b) receives, sends and manages information coming from and sent to the foreign similar institutions;
c) organizes the database regarding the international legislation and practice in the field;
d) elaborates the necessary documents for the participation of Office' representatives to the seminars, international conferences, experience exchanges, in collaboration with the other specialized directorates and supports the accomplishment of the assistance programs from abroad.

(4) Economic - Administrative Directorate has the following main attributions:

a) ensures, according to law, the substantiations and elaboration of the draft of the Office budget of revenues and expenditures, and observes its execution;
b) elaborates bookkeeping reports, according to the law;
c) analyses and monitors the efficient spending of approved funds;
d) ensures the application of the legal provisions regarding the recruitment, employment and payment of the personnel;
e) ensures the acquisition, management and administration of fixed assets, inventory objects and other materials;
f) ensures the maintenance and the exploitation of auto stock;
g) exercises preventive financial control upon operations which are coming from, finishes or modifies the patrimonial relations;
h) organizes the inventory process of material and financial means of the Office;
i) takes part in the auction activity;
j) keeps and brings up-to-date job cards;
k) elaborates the documents and perform the necessary activities for employment, transfer and redundancy activities;

(5) Legal Bureau carries out the following main attributions:

a) ensures specialized assistance in relations of the Office with third parties;
b) represents the Office in the Courts of Law;
c) advises for legal compliance the administrative decisions of the Office;
d) presents and disseminates within the Office the legal provisions related to its activity.

(6) Internal Audit Department has the following main attributions:

(a) certifies, quarterly and annually, enclosing the audit report of the annual balance sheet and budgetary execution accounts subsequent to the verification

of the legality, concreteness and accuracy of the bookkeeping records, financial and management documents;
(b) examine the legality, regularity and conformity of the operations, identification of the errors, dissipation, incorrect-management and frauds and, on these basis, issuing of measure and solution proposals in order to recover the damages and to sanction the persons found guilty;
(c) supervise the regularity in decision making systems, planning, programming, organization, co-ordination, monitoring and control of the decision's accomplishment.
(d) evaluates the ecumenicity, effectiveness and efficiency of the use of the financial, human and material resources, made by the leading and operative systems in order to accomplish the objectives and the planned results.
(e) identification of the weakness of the leading and control systems, as well as the risks associated to such systems, programmes or, as appropriate, operations and measure proposals for correction and for decreasing the risks.

**Art.11** - Individual attributions, tasks and responsibilities of the Office's personnel shall be established in the job description documents, according to the Law no. 21/1999, as amended subsequently, and the present Regulation, and shall be signed by the employee and his direct boss.

## CHAPTER IV
## Recruitment, employment and promotion conditions of the personnel

**Art.12 -** Employment of personnel shall be carried out by competitions, according to the law.
**Art.13 -** In order to take part in competition the candidates shall fulfill cumulative the following conditions:
a) to have only Romanian citizenship;
b) to have an university degree issued by an economic or legal high educational institute, with minimum length of service according to the nomenclature of job positions for specialized personnel and auxiliary specialized personnel, provided in the Annex of the Government Emergency Ordinance No. 237/2000 and for the personnel which holds similar positions to those in budgetary system, with minimum length of service and studies established by the Board;
c) to have the exercise of the civil and political rights;
d) to benefit of a professional and intact moral reputation;
e) to have no conviction for any offence;
e) to be declared admitted to the medical and psychological examination.

**Art.14** The folder for the participation to the competition for employment within the Office shall include:
a) candidate's request;
b) university diploma for higher education graduates and for the high schools and professional schools graduates, as appropriate, the high school or professional school graduation certificate, original and copy;
c) copy of the military record, as appropriate;

d) curriculum vitae;
e) reference – letter of recommendation from the last job;
f) criminal record certificate;
g) medical record;
h) copy of the job records;
i) a statement on own responsibility that the candidate has not been judged or convicted in penal cases and he is not subject of a current investigation or penal procedure.

**Art.15 –** As of the date of employment the personnel of the Office will sign an engagement regarding the liability of not disclosing the information received during its activity, but only in case of a judicial procedure including a five years period after ending of the employment period.

**Art.16 -** The employed personnel of the Office cannot hold any job and cannot fulfill any position within the legal entities provided for in the art.8 of Law no. 21/1999, as subsequently amended, being simultaneously an employee of the Office.

## CHAPTER V
## The waging system and other rights of the personnel hired within the Office

**Art.17 -** (1) The waging system of the specialized personnel and the auxiliary specialized personnel is similar to that of the personnel of the juridical authority bodies, in accordance to the annex of the Government Emergency Ordinance No. 237/2000.
(2) The personnel of the Office, other than the specialized one, stipulated in para (1), will be paid in accordance with the legislation referred to personnel working in the ministries and other specialized bodies under the Government subordination.
(3) The basic indemnity and the basic salary are established based on the position held within the structure in which the personnel is employed.

**Art.18 -** The employed personnel of the Office has the right, every year, to a vacation and other holidays established for employees in the public sector according to Government Decision no. 250/1992 regarding vacation and other holidays for employees of the public sectors, special autonomous regies and budgetary units, republished, as subsequently amended.

**Art.19 -** (1) Members of the Office's Board, financial analysts who are attached or delegated, shall benefit of a daily allowance of 2% out of the basic indemnity, settlement of the accommodation expenses in tourism structures with facilities up to and including 3 stars category, as well as the train transport with first class, first class sleeping carriage, plain or other transportation means, by case.
(2) For the financial analysts, abroad traveling daily allowance, transport and accommodation expenses are given according to art.49 para (3) from Law no. 50/1996 on the waging and other rights of the personnel from the judicial authorities bodies, republished.

(3) The other categories of personnel benefit from rights of traveling abroad or within the country, as well as the right to be temporary attached, according to the provisions for public institutions personnel.

## CHAPTER VI
## Final Provisions

**Art.20 -** The Office has an auto park, including 8 vehicles, the maximum consumption being of 300 liters of gas /month /vehicle

# GOVERNMENT OF ROMANIA

## DECISION no. 1078/08.07.2004

**for the modification of the Regulation on the Organisation and Functioning of the National Office for the Prevention and Control of Money Laundering, approved by the Government Decision no. 479/2002**

Based on the provision stipulated in the art. 108 of the Romania's Constitution, republished,
The Government of Romania decides:

**Single article. -** The Regulation on the Organisation and Functioning of the National Office for the Prevention and Control of Money Laundering, approved by the Government Decision no. 479/2002, published in the Official Gazette of Romania, Part I, no. 382/05.06.2002, as amended subsequently, is modified as follows:

1. Para (4) of the article 3 shall include the following content:

„(4) The Office's staff is composed of specialty and auxiliary specialty personnel, formed of financial analysts, assistants to financial analysts, as well as contractual personnel which holds specific positions to the budgetary sector".

2. The Article 4 shall include the following content:

"Art. 4. – (1) The organizational chart of the Office is provided for in the annex, which is entirely part of the present Regulation. Within the directorates could be organized divisions, bureaus and departments, through the Order of the Office's President.

(2) The attributions of the Office's Board and that of the directorates are set up through Prime-Minister's Decision, based on the proposal made by the Office's President, and for the other departments, through the order of the Office's President, in accordance with the law."

3. Para (3) of the article 8, article 9 and article 10 are repealed.

4. The article 13(b) shall include the following content:

"b) to have an university degree issued by an higher education institute or to have a secondary education degree, as the case stands, according to the law."

5. The annex of the Regulation is modified and replaced with the annex of the present decision.

PRIME-MINISTER
ADRIAN NASTASE
Countersigned:
President of the National Office For Prevention and
Control of Money Laundering,
Iulian Ilie Dragomir
for Ministry of Public Finances
Maria Manolescu
Secretary of State

*Bucharest, Nr. 1078/08.07.2004*

# National Office for Prevention and Control of Money Laundering

## DECISION No. 657/ 20.12.2002

**approved by the Plenum of the National Office for Prevention and Control of Money Laundering on the following reporting forms: Suspicious Transactions Report; Report on cash operations exceeding the equivalent of EUR 10.000; Report on cross border transfers in and from accounts, for sums whose minimum threshold is the equivalent in ROL of EUR 10.000**

**Published in: Official Gazette No. 2/ 07.01.2003**

Having regard to the provisions, referred to in art. 3 para (9) of the Law no. 656/2002 on the prevention and sanctioning of money laundering based on art. 8 of the Regulation on the organization and functioning of the National Office for Prevention and Control of Money Laundering, approved by Government's Decision no. 479/2002,

**The Plenum of the National Office for Prevention and Control of Money Laundering decides:**

**Art. 1** – The Suspicious Transactions Report, the Report on cash operations exceeding the equivalent of EUR 10.000 and Report on international transfers in/from accounts for sums whose minimum threshold is the equivalent in ROL of EUR 10.000, as presented in the annexes no. 1, 2 and 3, are approved.

**Art. 2** – The present decision, together with the Annexes no. 1, 2, 3 and the Annex A, which are entirely part of the present decision, shall be published in the Official Gazette of Romania, Part I.

**Art. 3** – Starting with the publishing date in the Official Gazette of Romania, Part I, of the present decision, the reporting of data provided by Law no. 656/2002 on the prevention and sanctioning of money laundering shall be carried out using the forms presented in the Annexes no. 1, 2 and 3, by the natural and legal persons subject to the Law, on paper sheet or electronic support, in which case the legal regime of the electronic signature and electronic certificate should be respected.

**Art. 4** – Plenum's Decision of the National Office for Prevention and Control of Money Laundering no. 3/1999 on the approval of the Suspicious Transactions Report and the Report on deposit and withdrawals cash operations which exceed the equivalent of EUR 10.000, published in the Official Gazette of Romania, Part I, nr. 377 on 6 August 1999 shell be abrogated.

President of the National Office on Prevention and
Control of Money Laundering,
Ioan Melinescu,
Secretary of State

**ANNEX no.1**

*SUSPICIOUS TRANSACTIONS REPORT*

## CHAPTER I – General information on the Report and the identification of the reporting entity.

### I.0. General Information:

| | |
|---|---|
| Reporting date ...…...…….... | Registration no. at sender ……...……... |
| Reporting entity type …….. | |

### I.A. Authorised Legal or Natural person.

Identification data:

| | |
|---|---|
| Name…. ……. | Unique code…… |
| Juridical statute ……..……. | |
| Incorporation number with Commerce Register…..…….. | Fiscal code….. …….. |

Headquarters:

| | |
|---|---|
| County ……...……. | Locality ……..……... |
| Street…….……..| No.…….| District…… | |

Sub-unit where the reporting activity has been carried out :

| | |
|---|---|
| Branch …….. …….. ……..... | |
| County …….…… | Locality ……..……... |

### I.B. Natural Person.

Identification data:

| | | |
|---|---|---|
| Name…….....….. | Surname ……..... | |
| Identity card type ..... | Series ..……... | No. doc… …….……..... |
| Issued on ……... | By…….……. | |
| Personal digital code ….. ……..……... | | |

Residence :

| | | |
|---|---|---|
| Country…..……... | County……..| Locality …….. | |
| Street…….……| No…….| District …… | | |

## CHAPTER II – Customer's identification data.

### II.A. Romanian or Foreign Legal Person.

Identification data:

| | |
|---|---|
| Name …..…….. | |
| Juridical statute ……..……. | |
| Incorporation number with Commerce Register ……..... | Fiscal code... …….. |

Incorporation place (for foreign legal persons):

| | |
|---|---|
| Country…….....…….. | Locality…….……...... |

Headquarters:

| | | |
|---|---|---|
| Country…..……... | County……..\| Locality …….. | |
| Street…….……\| No……\| District…… | | |

Identification data of the legal representative:

| | |
|---|---|
| Name …….....…. | Surname ……...... |
| Personal digital number…… …….……... | |

### II.B. Romanian or Foreign Natural Person.

Identification data:

| | | |
|---|---|---|
| Name …….....……. | Surname …….....| |
| Date of birth…….. …..... | Place of birth …… ……..... | |
| Citizenship ……\| Resident / Non-resident …… | | |
| Identity Card Type …….. | Series ……..… | No. doc. …….……..... |
| Issued on …….. | By ……. | |
| Personal Digital Number …….……... | | |

Domicile or residence:

| | | |
|---|---|---|
| Country ..…….... | County ……..\| Locality …….. | |
| Street…….……\| No……\| District…… | | |

Phone / fax :

| | |
|---|---|
| Phone no. ……. | Fax ……..……... |

### II.C. Information on client's accounts and sub-accounts – legal person or natural.

| | |
|---|---|
| Account's type ……...…..…… | Total number of accounts …… ..... |

II.C.1 Details on accounts and sub-accounts :

| | |
|---|---|
| Accounts…….……. ... ……. | Sub-accounts ...…… |

### II.D. Information on customer's connexions with other natural or legal persons.

| | |
|---|---|
| Connexion type …… ….……. | Total no. of connexions …… |

**II.D.1. Details on legal persons being in relation with the customer:**

| |
|---|
| Name …….. |
| Juridical statute …….…… |
| Fiscal code ……..... …….. |

**II.D.2. Details on natural persons being in relation with the customer:**

| | |
|---|---|
| Name ……..... | Surname …….... |
| Personal digital number…….…….……. | |

**II.E. Significant operations carried out in the last 12 months.**

| | |
|---|---|
| Operation's type ……..……. | Number of operations …… |
| Total sum ……. | |

**II.F – Person performing the transaction.**

Identification data:

| | | |
|---|---|---|
| Name ..…….....…. | Surname …….....**.....** | |
| No. of the power of attorney document … ……. | | |
| Type of the Identity Card **.....** | Series ……...… | No. doc. ……..…….…..... |
| Issued on …… | By ……..…… | |
| Personal digital code …… ……..... | | |

Domicile / Residence:

| | |
|---|---|
| Country…….……. | County..……..\| Locality …….. |
| Street…….……\| No…….\| District…… | |

## CAPITOLUL III – Data on transaction and accounts involved.

**III.A. Description of the transaction:**

| | |
|---|---|
| Transaction date.……\| Sum involved……\| Foreign currency ……... | |
| Transaction type ……. \| Transacion's stage ……..……\| Modality of payment ……... | |
| Transaction's nature ... ……... | Transaction's object ……. |
| Account's type ……\|Accounts used……\| Sub-accounts …….. | |

**III.B. Data on sender, intermediary or beneficiary of the transaction performed with the person referred to in the chapter II (Legal person).**

Identification data:

| | |
|---|---|
| Name …….. | |
| Juridical statute ……..…..……. | |
| Incorporation number with Commerce Register ……..….... | Fiscal Code .... …….. |

Headquarters :

| | |
|---|---|
| Country …….……. | County……..\| Locality …….. |

| Street…….……| No…….| District …… |
|---|

**III.C. Data on ordering customer, intermediary or beneficiary of the transaction performed with the person referred to in the chapter II (Natural person).**

Identification data:

| Name ……..……..…….. | | Surname ……..... |
|---|---|---|
| Type of the Identity Card …….. | Series ……..… | No. doc. …….……..... |
| Issued on …….. | By ……. | |
| Personal digital code…..……..……... | | |

Residence:

| Country…...…….. . | County ……..| Locality …….. |
|---|---|
| Street…….……| No…….| District …… | |

**III.D. Description of the unusual/ suspicious aspects.**

| Description of the operation…….…..**.....**<br>**.....**<br>**.....**<br>**.....**……<br>……<br>…… |
|---|
| Description of the aspects deemed to be suspicious**.....**<br>**.....**……<br>**.....**<br>**.....**……<br>……<br>……<br>…… |

Note:

*Chapter I*

- It is to be filled in only one of the sub-chapter I.A or I.B depending on the juridical statute of the reporting person.
- *Registration number at the sender*, in case of a suspicious transaction report on paper base will be the registration number of the report. For the reports on electronic base, registration number at sender is a sequence number (starting with 01), which identify uniquely the report for a version of the application and for a certain reporting entity.
- Admissible Values for the headings:
  - *Type of the reporting entity;*
  - *Juridical statute;*
  - *Identity card type*

  are listed in the respective tables in the Annex A.

*Chapter II*

- The completion of all headings of the chapter II is compulsory. Sub-chapters shell be completed distinctively for each person/account/operation involved in the suspicious transaction.
- In the heading *Resident / Non-resident* can be completed 2 values only: '**R**' – for resident or '**N**' – for non-resident.
- Admissible Values for the headings:
  - *Juridical statute;*
  - *Identity card type;*
  - *Account type;*
  - *Connexion type;*
  - *Operation type*

  are listed in the tables of the Annex A.

*Chapter III*

- All headings of the chapter III are compulsory and shall be completed as many times as needed, if the suspicious operation is made of more transactions.
- At the heading *Transaction type* can be completed 2 values only: '**D**' - debit or '**C**' – credit.
- At the heading *Transaction stage* can be completed 2 values only: '**E**' - executed or '**N**' – non-executed.
- Admissible values for headings:
  - *Foreign Currency;*
  - *Payment Modality;*
  - *Nature of the transaction;*
  - *The object of the transaction;*
  - *Account type;*
  - *Juridical statute;*
  - *Identity card type*

  are listed in the tables of the Annex A.

**Mention:**
For submitting the reports on electronic support, NOPCML will give in hand of the reporting entities the application Data Entry and the Manual for its use.

Legal reporting person:

Name:
Address:
Fiscal code:
Incorporation number with Commerce Register:

**ANNEX No. 2**
Reporting date:

Exchange Rate Euro BNR:

# REPORT
## on operations in cash which exceed the equivalent of EUR 10.000

| No | Branch | Customer Type | **Information on customer (owner of the account)** | | | | | | | | | | Date and place of birth | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Name* | Surname* | ***Address*** | | | | | | Identity Card | Customer code | Date | Country | Locality |
| | | | | | Country | County | Locality | Street | No. | District | | | | | |
| **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** |

| ***Information on the person which performs the transaction*** | | | | | | | | | | **Account** in which is performed the operation | Date of the operation | Kind of the Operation |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Name | Surname | ***Address*** | | | | | | Identity document | Personal digital number | | | |
| | | Country | County | Locality | Street | No | District | | | | | |
| **16** | **17** | **18** | **19** | **20** | **21** | **22** | **23** | **24** | **25** | **26** | **27** | **28** |

| Purpose of the operation | Foreign currency code | Transaction's sum | Equivalent Euro | Observations |
|---|---|---|---|---|
| **29** | **30** | **31** | **32** | **33** |

*For the legal persons, in the column 3 shall be filled in *name* and shall not be filled in the column 4.

**ANNEX NO. 3**

# REPORT
## on cross border transfers of sums into and from accounts whose minimum threshold is the equivalent of Euro 10.000

## CHAPTER I – General information on report, reporting entity and foreign entity.

### I.A. General information on report:

| | |
|---|---|
| Issuing date ...…...…….. | Registration no. at sender …...……... |

### I.B. Reporting entity:

Identification data:

| |
|---|
| Name …. …….. |
| Identification date (fiscal code or that in BNR's codification) …… |
| Sub-unit ….. ……\|Sub-unit's code . …….. …..... |

### I.C. Foreign entity:

Identification data:

| |
|---|
| Name …. …….. |
| Country…….. |

## CHAPTER II – Information on the customer of the reporting entity (the owner of the account).

### II.A. Romanian or foreign legal person.

Identification data:

| | |
|---|---|
| Name …..…… | Unique code…… |
| Incorporation no. with Commerce Register ……..... | Fiscal code.. …….. |

Place of incorporation (for foreign legal persons):

| | |
|---|---|
| Country…….....…. | Locality……... |

Headquarters:

| | | |
|---|---|---|
| Country…..……... | County……..\| Locality …… | |
| Street…….……\| No…….\| District… | | |

Identification data of the legal representative:

| | |
|---|---|
| Name …….....… | Surname …….....**.....** |
| Personal digital number …….…….. | |

**II.B. Romanian natural or foreign person.**

Identification data:

| | | |
|---|---|---|
| Name …….....…….. | Surname …….....** | |
| Personal digital number…… | | |
| Identity card type…….. …….. | Series……..… | No. doc. …….....** |
| Issued on …….. | By…… | |
| Citizenship…….| Resident / Non-resident. …… | | |

Domicile or residence:

| | | |
|---|---|---|
| Country ...……... | Country……..| Locality …….. | |
| Street…….……| No…….| District… | |

**II.C. Information on account.**

| |
|---|
| Account's type ( 0=Individual; 1=Joint holding; 2=Legal person)…....….…… |
| Account….. ……... |
| Account's type ……... |

## CHAPTER III – Information on the customer of the foreign entity.

**III.A. Legal person.**

Identification data:

| |
|---|
| Name…..…….. |

**III.B. Natural person.**

Identification data:

| | |
|---|---|
| Name …….....…….. | Surname …….....** |

**III.C. Information on account.**

| |
|---|
| Account ……... |

## CHAPTER IV – Person performing the transaction (representative).

Identification :

| | |
|---|---|
| Name ..…….....…. | Surname |

| | |
|---|---|
| | …….…. |
| Personal digital number ……<br>…….…… | |
| Type of the power of attorney document ……..…….. | No./Date……... |
| Type of the identity card **.....** | Series……..… No. doc. ……..…..... |
| Issued on …… | By……..…… |

Residence :

| | |
|---|---|
| Country…..…….…. | County……..\| Locality…... |
| Street…….……\| No…….\|<br>District…… | |

## CAPITOLUL V – Data on transaction.

### V.A. Description of the transaction:

| |
|---|
| Transaction date ……\| Sum involved ……\| Foreign currency……... |
| Transaction type (D/C)……. ……\| EURO equivalent …… |
| Details on operation …….. |

### V.B. Observations.

| |
|---|
| ……..……..….....**.....**<br>**.....**<br>**.....**<br>**.....**.....……<br>……<br>……..…..<br>**.....**<br>**.....**<br>.....…… |

# NATIONAL BANK OF ROMANIA

## NORM NO.3/26.02.2002
### REGARDING KNOW-YOUR-CUSTOMER (K.Y.C.) STANDARDS

Under the provisions of article2 (2) and of article 26(2) of the Law no. 101/1998 regarding the Statute of the National Bank of Romania, with subsequent amendments and supplements, and of article 45 and article 55 of the Law no. 58/1998 - the Banking Law, with subsequent amendments and supplements,

Taking into consideration the provisions of the Law No. 21/1999 regarding the prevention and sanction of money laundering, as well as the necessity of reducing the reputational*, operational, credit and liquidity risks, accordingly to the requirements of the law, in order to protect bank's safety and stability, and the integrity of the banking system,

*) The potential of the adverse publicity regarding a business practices of a bank and/or of the person being in connection with it – shareholders, business partners, etc. – whether accurate or not, will cause a loss of confidence in the integrity of the bank.

the National Bank of Romania issues the present norm:

## CHAPTER I
## GENERAL DISPOSALS

**Article 1**
(1) The present norm applies to banks, Romanian legal entities, and provides the basic framework for issuing their own "know-your-customer" policies and procedures as an essential part of a sound risk management and efficient internal audit systems.
(2) These norms should apply accordingly to the branches of the foreign banks in Romania.

**Article 2**
In order to ensure the carrying out of the banking activities in compliance with the legal requirements, including with the legislation regarding the Anti–Money Laundering as well as the rules of a prudential and sound banking practice, banks shall have in place efficient "know-your-customer" policies and procedures, further called *know-your-customer* (KYC) *programmes*, to promote high ethical and professional standards and to prevent the bank from being used in an illegal or criminal activity performed by its customers.

**Article3**

(1) Under the present norm, the term *customer* includes the following meanings:

a. any individual, legal entity or entity without juridical personality that keeps an account with a bank through which transactions concerning funds received or distribution are carried out;

b. any individual, legal entity or entity without legal personality on whose behalf an account is maintained;

c. any individual, legal entity or entity without juridical personality as beneficial owner of financial transactions in which the bank is involved, if can generate a significant reputational risk or a risk of another nature to the bank.

(2) The meaning of client should have a large extend, that includes, without being limited:

a) any direct or indirect beneficial owner of a current, deposit, credit or of any other account through which transactions concerning funds received or distribution are carried out;

b) any person or entity who is the real beneficiary of the transactions performed through professional intermediaries, such as investment companies, pension funds or other investment administration companies,

c) corresponding banking;

d) any person conferred with power of attorney to conduct transactions on customer behalf.

**Article 4**

(1) The know-your-customer programmes shall consider all the bank activities related to the customers' transactions including, without being limitative, the following:

a) opening of current, deposit, savings, credit and card accounts;

b) opening of securities accounts;

c) renting of safe-deposit boxes;

d) the execution of transactions with securities or other financial instruments, foreign currency, as well as metals and precious stone exceeding the equivalent of Euro 10,000;

e) cash transactions exceeding the equivalent of Euro 10,000;

f) granting of loans and operations having commercial effects.

(2) Cash transactions refer to transactions carried out at the a bank's teller window, such as: currency exchange, purchase and sale of precious metals, cash subscriptions to bank "cash bonds", cash sale of travellers cheques, cashing of cheques, and other transactions.

(3) The provisions of the paragraph 1 are not applicable in case of opening accounts with a view to paying up capital stock in connection with the formation of a corporation/ company, except for the case the bank has cause to suspect money laundering.

**Article 5**

The requirements of the KYC standards are applicable in the cases of the transactions when bank is involved too, and can generate for it a significant

exposure to a reputational risk or another kind of risk, resulting from its contractual partnership provisions, or from any other individual or entity clearly related to that transaction.

## CHAPTER II
## ESSENTIAL ELEMENTS OF KYC STANDARDS

### Section 1 – The KYC standards

**Article 6**
Each bank shall set its own KYC standards taking into account the nature, size, complexity and extension of its activity, accordingly to the risk level associated to all types of customers provided with banking services by the bank.

**Article 7**
The KYC programmes shall include, at least, the following:

a. customer acceptance policy;
b. customer identification procedures;
c. up-to-date record-keeping procedures;
d. on-going monitoring of accounts and transactions in order to detect the suspicious transactions, and the procedure of reporting them;
e. modalities of pay attention to the transactions to and/or from jurisdictions that don't have proper regulations on anti–money laundering;
f. procedures and control systems of the KYC programme's implementation and evaluation;
g. on-going employee-training programme so that banks employee/staff is adequately trained in KYC procedures.

**Article 8**
The KYC standards shall be established in a writing form and shall be approved by the board of directors of each bank. These standards shall be learned by all staff involved and the board of directors on regular basis shall adjust the evaluations of the effectiveness of these programmes accordingly.

### Section 2 – The customer acceptance policy

**Article 9**
(1) Banks shall develop clear customer acceptance policies and procedures, including at least a description of the acceptable types of customers, banking products and services types which can be provided to each category of customers, graduated customer acceptance policies and procedures accordingly to the risk associated to different categories of customers, including a description of the types of customers that are likely to pose a higher than average risk to a bank.

(2) Bank's decisions to enter into business relationships with customers and to provide them banking products and services should be taken exclusively considering the customer's quality, and not the bank's high credit risks exposure. When issue the customer acceptance policies and procedures the bank should take this into account.

**Article10**
Banks that provide complex banking services, known as *private banking*, shall develop policies that require more extensive due diligence for their high risk customers; all new customers included in this category shall be approved both within the organisational chart that manages this type of customers, and by at least one person charged with duties in the customers' risk management field.

**Article11**
Decisions to enter into business relationships with higher risk customers shall be taken exclusively at senior management level, or, if the case, at the executive management level in accordance with the responsibilities given.

## Section 3 – Customer identification

### 3.1 General principles

**Article12**
(1) Banks shall establish a systematic procedure for verifying the identification of new customers and those acting on their behalf, and shall never enter a business relationship until the identity of a new customer is satisfactorily established.
(2) Banks shall never agree to open and manage anonymous accounts, for which the identity of the holder is not known and recorded accordingly.

**Article13**
Banks need to obtain all information necessary to establish the identity of each new customer and the purpose and intended nature of the banking services which will be provided to it's customer. The extent and nature of the information depends on the type of the prospective applicant – individual, corporate – and the expected nature and size of the transactions carried out through the bank.

**Article14**
Customer identification policies and procedures shall be equally applicable both in the cases of opened accounts and maintained on customer behalf, and in the case of non-nominative accounts for which the identity of the holder, known by bank, is replaced in records by a numerical code or by a code of another nature, in view of ensuring of a very high level of confidence.

**Article15**
In the case of savings and deposit accounts, banks must verify the identity of any person who deposit or withdraws amounts exceeding the equivalent of Euro 10.000.

**Article16**
The bank shall verify the identity of the customer/customers when entering into transactions, (stipulated at the article 4, par. 1, letters d. and e.) below the limit of the equivalent of Euro 10,000, if there are suspicions that the transaction has been split up with the purpose of avoiding the identification requirements.

**Article17**
If the bank has cause to suspect money laundering, it has to verify the identity of the customer, regardless of value of the transaction or exceptions to identification requirement, stipulated in article 4, paragraph 3.

### *3.2. General identification requirements*

**Article18**
(1) Banks shall verify/establish the identity of the customer by examining an official identification document or other identification documents and shall put on record the data required to be kept on file for their customers, including the occasional ones.
(2) Special attention shall be exercised by banks, in the case of non-resident customers and on the customers who are unable to present themselves for interview.

**Article19**
Banks shall take steps necessary to verify the information provided by the customer within the customer identification procedures. If necessary, banks verify the identity of the customer by obtaining confirmation of the domicile indicated, either through an exchange of correspondence, direct observation of the location, and/or dialling the customer telephone number, checking the invoice or by any other method.

**Article 20**
(1) In the case of customers - individuals, banks shall require and obtain at least the following information:
a) name and surname and, if the case, pseudonym;
b) permanent residential address;
d. date and place of birth;
e. name of employer or nature of self-employment/business;
f) source of funds;
g) specimen signature.

(2) Banks shall verify the information against original documents of identity issued by an official authority, such as identity cards, passports, documents that are most difficult to obtain illicitly and/or to counterfeit. This official document shall include the owner's photograph, his/her signature, and if necessary, the owner's description.
(3) In order to classify the client into one of categories set up by the bank and in order to apply the reporting obligations according to the law, additional information that can be requested should refer to nationality or country of origin of the client, public or political function or other information.

**Article21**
(1) The identification of customers, legal entities or entities without juridical personality must be established by means of an extract from a public register and the documents upon which the registration of the company was based. These documents will be provided either by the customer or by a public register, or by both sources. While there are no registration requirements, the identification will be made on the basis of the incorporation documents, including the business license and/or the audit reports.
(2) The customer identification procedures shall at least include the following:

a) to verify the legal existence of the customer, by obtaining from the Commercial Register or from another public register, proof of incorporation, including information concerning the customer's name, legal form, permanent residential address, type and nature of the activity, the administrators/directors' identity and provisions regulating the power to bind the entity;

b) to verify that any person purporting to act on behalf of the customer is so authorised and identify that person.

**Article22**
(1) In order to fulfil identification requirements, banks may ask for additional information related to their financial statement, entity structure, identity of the individuals on whose behalf the transactions are conducted by the entity in cause.
(2) In order to verify some information provided by the customer, banks might use the third party's certification.

**Article23**
(1) Banks shall keep records on customer identification, including photocopies of identification documents and/or of other documents, so as to provide at least the information stipulated in article20 paragraph (1) and article21 paragraph (2), as well in article11 and article44 letter c), measures needed to identify, analyse and effectively monitor higher risk customer.
(2) Banks will ensure the internal control department and independent auditor access to the evidence kept.

### *3.3 Specific identification issues*

**Article24**

(1) Banks shall take all the necessary measures to obtain information about the true identity of the persons on whose behalf an account is opened or a transaction conducted.

(2) - If there are any doubts as to whether these customers (article24. par.1) are acting on their on behalf, banks shall exercise adequate due diligence in establishing the identity of the real beneficial owner. In this respect, they must require its customers to declare the identity of the beneficial owner in a form as the one attached as Annex (Establishment of the Beneficial Owner's Identity) to the present norm.

**Article25**

The banks have the right to print their own declaration (establishment) form that reflects their own particular requirements in one or as many international languages they want. These forms must contain at least the complete text of the sample form attached as Annex.

**Article26**

Banks shall be suspicious about the true identity of the beneficial owner in the following situations:

a) when a power of attorney is conferred on someone who clearly would not have sufficiently close links to the customer, in order to conduct transactions using his account;

b) when the financial standing of the customer wishing to carry out a transaction is known to the bank, and the funds or assets submitted or about to be submitted are disproportionate to declared customer's financial standing;

c) when the bank notices more unusual situations during its relationship with the client.

**Article 27**

The bank shall ask customer to submit a declaration about the identity of the true beneficial owner, in a form as the one attached as Annex, in the following cases:

a) If the amount of a cash transaction exceeds the equivalent of Euro 10,000;

b) When the bank enters into business relations with its customers through correspondence or another way that does not need the customer's presence at bank.

**Article 28**
If serious doubts persist about the accuracy of the customer‘s written declaration and cannot be dispelled through further clarification, the bank shall refuse to enter into a business relationship or to execute the transaction.

**Article 29**
In the case of opening and maintaining joint accounts (hold by many owners), banks shall require and keep records on full lists of the identity of beneficial owners of the account.

**Article 30**
In the case of opening accounts on behalf of another person, acting as an intermediary – mandatory, trustee, nominee, funds administrator, custodian, legal guardian or other intermediary – the bank shall require and obtain the satisfactory information and documents about the identity of the intermediary and the beneficial owners (upon whose behalf they are acting), as well as details of the nature of the trust.

**Article 31**
(1) In the case of opening joint accounts managed by professional intermediaries – management companies– on behalf of entities such as mutual funds, pension funds or other entities, as well as joint accounts managed by lawyers or brokers, banks shall consider the followings:

a) In the case of accounts opened on behalf of collective securities investment bodies with more than 50 investors as beneficial owners, the information about beneficial owners' identity shall be recorded only for that investors who hold, directly or indirectly, minimum of 5 % of the body's assets;

b) In the case of accounts opened on behalf of collective securities investment bodies with less than 50 investors, the bank shall require information about all beneficial owner's identity;

c) In the case of accounts opened on behalf of an intermediary, where there are "sub-accounts" which can be attributable to each customer, the bank shall apply the customer identification procedures stipulated in the present norm for each beneficial owner.

(2) Banks shall accept the opening of such accounts, only if, they are able to determine that the intermediary applied customer identification procedures in a satisfactory manner. At the same time, intermediary must own an adequate system to allocate the assets on each beneficial owner. Banks shall apply the criteria stipulated in article 32 in order to evaluate the intermediary's procedures.

(3) Bank shall not accept entering into relationship with an intermediary, if this one cannot provide the requested information to the bank as regards the beneficiaries or non–equivalent standards to these norms are not applying for the intermediary.

**Article 32**

(1) Accepting a new customer under the identification data provided by other banks or by a third party (who is an intermediary between the bank and customer), banks shall be ensured about the quality of the customer identification procedures used by the intermediary. In order to evaluate the procedure's quality, the bank will consider the following requirements:

a) to be ensured that the intermediary's procedures comply with the minimum standards imposed by KYC procedures, and that they are at least as strictly as those implemented by bank;

b) to conclude an agreement with the intermediary through which the bank is allowed to verify the intermediary's KYC standards;

c) to be ensured that the intermediary have the obligation to provide the bank with all the information and identification documents processed by its own identification procedures.

(2) The ultimate responsibility for knowing customers always lies with the bank.

**Article 33**

(1) In the case of business relations entered into through correspondence or modern means of telecommunications – telephone, e-mail, internet – banks shall apply equally effective identification procedures and on-going monitoring standards for non-face-to-face customers as to those available to present themselves to the bank.

(2) In the case of such relationships, the bank shall verify the accuracy of the address, and of the telephone number provided by the means stipulated in article 19, or by any other means considered to be appropriate for the bank. In order to identify the customer, bank will require the needed documents and will record them accordingly, on the customer's first visit to the bank.

(3) In order to a better identification of this category of customers, banks shall take some measures, such as:

a) all documents forwarded to bank, including the signature specimen, need to be certified by a branch of a bank or by a trustee, especially in the case of non-resident customers;

b) additional documents may be required;

c) an introduced customer may be accepted, if the intermediary as introducer meet the requirements stipulated in article 32;

d) the requirement that the first payment to be carried out on behalf of the customer through an account opened with another bank that comply with similar customer identification and verification standards.

**Article 34**

Banks shall pay a special attention in the cases it enter into corresponding relationships or continue such relationships with a bank recorded in a jurisdiction which was identified as not granting assistance in the money laundering field.

## Section 4 – On-going monitoring of the customer

### Article 35
On-going monitoring of customer identification process includes at least the following activities: permanent up-to-date customer identification papers, re-evaluation on regular bases of the quality of the identification procedures applied by the intermediaries and on-going monitoring of transactions and accounts in order to determine and report suspicious transactions in compliance with the bank's internal procedures.

### Article 36
(1) Banks shall review the information available on existing customers on regular bases and keep up-to-date the records since the beginning of the business relations.
(2) Any subsequent amendment of the provided information shall be verified and recorded accordingly.
(3) If significant changes to the customer (company) structure, legal entities or other entities without juridical personality or their holders, occur subsequently, further checks shall be made by bank.
(4) Either bank is aware that it lacks sufficient information about an existing customer or there are signs that bank is suspecting provided information not to comply with the reality, bank shall take steps to ensure that all relevant information is obtained as quickly as possible.
(5) Bank shall take necessary measures to obtain all relevant information as soon as possible, whenever there are gaps in information about the client or whenever there are some suspicions or the bank suspects that the information is not accordingly to the real situation.
(6) In case that requested information cannot be provided or consequently it is noticed that the information provided by the client is not accordingly to the real situation, bank shall do all diligences to terminate the relations with the client, and, depending on situation, bank will report the case to the competent authority and to National Bank of Romania.

### Article 37
Banks shall undertake regular reviews of the quality of identification procedures applied by the intermediary in order to be ensured that these are in accordance with the requirements stipulated in the present norm.

### Article38
(1) Banks shall ensure monitoring of the client's activity through an on–going follow up of the transactions performed by the client into all his accounts, nevertheless the types of accounts or territorial units of the bank.
(2) The program shall be equipped with different levels of on-going monitoring of transactions carried out through accounts that have to be in accordance with the levels of risks associated to the different categories of customer.

**Article39**
In order to ensure an efficient on-going monitoring of transactions and accounts, banks shall understand the customer activity, in order to identify the unusual performed transactions through it banking accounts.

**Article40**
The identification procedure of the normal and expected activity of the customer shall take into consideration the type of account opened with the bank. In this respect, bank shall made a customer classification (in many categories) regarding factors such as:

a) the account type;

b) the transactions type carried out through different account types;

c) the transactions number and volume carried out through an account;

d) the risk of an illicit activity associated to different types of accounts and transactions carried out through accounts.

**Article 41**
For all accounts, banks shall have adequate systems in place to detect unusual or suspicious transactions. This can be done by establishing limits for a particular class or category of accounts. Particular attention shall be paid to transactions that exceed these limits. They may include normal transactions that can be carried out through particular types of accounts, such as: value limits on each type of transaction, customer or account, activity field of legal entities or another entities. In this case, the on going monitoring shall focus on the transactions that are not consistent with the established limits.

**Article 42**
(1) The program shall include an adequate system to detect suspicious transactions, and reporting procedures of these transactions to a person designated under the provisions of article47 paragraph 2, and competent authorities. Bank shall focus on the certain types of transactions that are not consistent with the normal patterns of activity and isolate the higher risk transactions for a later evaluation. The need to pursue suspicions depends on the size of the assets and incomes (turnover), pattern of transactions, economic background, reputation of the country of origin, plausibility of the customer's explanations.

(2) The suspicious transactions may include:

a) transactions that are not consistent with the normal patterns, including the ones due to unusual frequency of the withdrawals or deposits operated into account;

b) complex transactions of significant value implying deposits and withdrawals of large amounts of money;

c) external transfers or other transactions that do not make economic, commercial or legal sense, including external transfers that are not consistent with the statutory activity of the customer or that are ordered by the customers that are not relevant to the statutory activity.

(3) The purpose and circumstances of such transactions shall, as far as possible, be examined under additional documents required to the customer in order to justify the transaction, the findings established in writing, and be available to the subsequent verifications. The transactions shall be reported to the designated person under the provisions of article 47 paragraph 2.

**Article 43**

Most, or, if necessary, all transactions carried out by higher-risk customers through their accounts shall be effectively monitored. In establishing the higher-risk customers shall be considered the following:

a) type of customer – individual or legal entity;
b) country of origin;
c) important or public position held;
d) accounts associated to the customer;
e) specific of the activity carried out by the customer;
f) funds source;
g) other risk factor.

**Article 44**

For the potential higher risk customers:

a) banks shall ensure that they have adequate management information systems to provide managers and compliance officers with timely information needed to identify, analyse and effectively monitor higher risk customer accounts. The implemented systems shall be focused at least on: missing account opening documentation, transactions made through a customer account that are unusual, and aggregations of a customer's total relationship with the bank;

b) senior management of a bank in charge of private banking business shall know the personal circumstances of the bank's important customers and be alert to sources of third party information;

c) high value transactions of these customers shall be approved by the bank's board of directors, or when necessary, by the executive management.

**Article 45**

(1) Banks shall refuse to execute suspicious transactions, and transactions against the law or the ones that can not be justified accordingly.

(2) Banks shall report the suspicious transactions to the National Bank of Romania – to the Supervision Department. The report shall include the customer's identification elements, the amounts and types of currencies involved in the transaction, the justification of the transaction, the reasons for being considered a suspicious transaction and any other information relevant to the bank. If banks suspect that funds stem from criminal activities, they shall report promptly their suspicions to other competent authorities.

## Section 5 – Risk management

### Article 46

(1) Each bank shall have adequate policies and procedures in place to ensure the implementation of an efficient KYC programme. In this respect, under the provisions of internal regulation, at least the followings shall be ensured:

a) segregation of duties;

b) routines for proper management, systems, and controls oversight;

c) strategies for an on-going employee-training programme so that bank staff is adequately trained in KYC procedures.

(2) The new bank's products and services shall be evaluated with a view to establishing their associated potential risk, including the risk of being used in criminal or fraud activities.

### Article 47

(1) Banks shall fully establish the responsibilities, by internal rules and regulation, so that to ensure that the appropriate policies and procedures are used efficiently. Banks shall have clear written procedures, communicated to all personnel, for staff to report suspicious transactions to a specified manager.

(2) Bank shall appoint a senior officer with explicit responsibility for the co-ordination and on-going monitoring of the established procedures.

### Article 48

(1) Banks' internal audit procedures shall have important responsibilities in providing an independent evaluation of the bank's own policies and procedures, including the legal and regulatory requirements.

(2) The internal audit shall play an important role in evaluating on regular basis the efficiency of the established policies and procedures, including employee training performance, and to remove the founded deficiencies and to observe the manner in which conclusions and proposals made are solved.

(3) The staff's responsibilities in charge with the internal audit shall include on-going monitoring of staff performances through sample testing of compliance and review of exception reports to alert senior management or the board of directors if it believes management is falling to address KYC procedures in a responsible manner.

(4) Management shall ensure that internal audit department is staffed adequately with individuals who are well versed in such policies and procedures.

### Article 49

(1) Banks must have an ongoing employee-training programme, so that bank staff is adequately trained in KYC procedures. The timing and content of training for various sectors of staff will need to be adapted by the bank for its own needs.

(2) Training requirements shall have a different focus for new staff, front-line staff, compliance staff or staff dealing with new customers. New staff should be educated in the importance of KYC policies and the basic requirements at the bank. Front-line staff members who deal directly with the public should be trained

to verify the customer identity for new customers, to exercise due diligence in handling accounts of existing customers on an ongoing basis and to detect patterns of suspicious activity.
(3) Regular refresher training, at least once a year or any time when necessary, should be provided to ensure that staff is reminded of their responsibilities and is kept informed of new developments in this field, so to ensure a constant implementing of the established programmes.

## CHAPTER III
## IMPLEMENTATION OF KYC STANDARDS IN A CROSS-BORDER CONTEXT

**Article 50**
(1) The bank shall ensure the implementation of the KYC standards in all its territorial units and subsidiaries, domestic and international, and have a routine for testing on regular basis the compliance against both the requirements stipulated in the present norm and the host country KYC standards in order for their programmes operate effectively globally.
(2) The bank shall have a procedure for reviewing the vulnerability of reputational, operational, concentration risks, and the compliance with the requirements of the law in all its territorial units, and implement special measures of the bank's safety, if necessary.
(3) The existent records about customers, at the level of each territorial unit and subsidiary, shall be kept accordingly and available, when necessary, to the internal audit or the National Bank of Romania inspections.

**Article 51**
If the host country's laws and regulations– especially banking secrecy provisions – prohibit the implementation of the requirements stipulated in the present norm, territorial units and overseas subsidiaries of the bank would have to comply with host country standards, but they shall make sure parent bank and the National Bank of Romania (as home country supervisor) are fully informed of the nature of the difference.

## CHAPTER IV
## SUPERVISION OF COMPLIANCE WITH THE REQUIREMENTS OF KYC STANDARDS

**Article 52**
(1) The board of directors of each bank shall be fully committed to an effective strategy of KYC programmes and implement a clear policy, communicated to all personnel, of the ethical and professional behaviour in the customer-bank relationship.

(2) Decisions, to carry out of transaction to potential higher-risk customers, and any other kind of transaction in which bank is involved and which have a higher-risk level associated to, shall be taken by the board of directors of the bank or, if the case, by the senior management. Decisions shall be taken based on the adequate documentation and analyses of all the circumstances of certain transaction in order to determine the associated risks and include, if necessary, additional protection measures to ensuring a decrease of these risks.

**Article 53**
The senior managers and the other members of the board of directors shall be responsible for:
a) issuing and implementation of an efficient KYC programmes;
b) ensuring an adequate training for the involved staff;
c) exercising the control over the established programs and efficiency of the policies, procedures and systems implemented;
d) carrying out or involving bank in transactions without a sound analyse made under the established standards, of the risks associated to the respective transactions;
e) carrying out or involving the bank in transactions when they knew or shall know that these have an important risk for the bank by the jeopardizing the creditworthiness and viability of the bank by an inadequate funds management of the bank;
f) non-observance of other provisions stipulated in the present norm.

**Article 54**
Banks undertake to ensure that supervisors have access to all the documents about customers and transactions carried out through their accounts, including any analyse that bank perform in order to detect unusual or suspicious transactions, or to determine risk level associated to a transaction in which the bank is involved.

**Article 55**
(1) For non-observance of the provisions of the present norm, the National Bank of Romania shall apply the sanctions stipulated in article69 of the Law nr.58/1998 – the Banking Law and shall dispose, when necessary, remedy measures, under the provisions of article70 of the same law.
(2) The application of the sanctions by the National Bank of Romania does not remove the penal, civil or other kind of responsibility, if the case, of the persons sanctioned.

## CHAPTER V
## FINAL AND TRANSITORY PROVISIONS

**Article 56**
(1) Banks shall maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly

with information requests from the competent authorities. Such records must be sufficient to permit reconstitution of individual transactions – including the amounts and types of currency involved if any – so as to provide, if necessary, evidence for prosecution of penal facts (criminal behaviour).
(2) The records on customer identification – copies or records of original identification documents – accounts files and business correspondence shall be kept, by bank, for at least five years after the account is closed. All these documents shall be available, under the provisions stipulated by law, to domestic competent authorities in the context of relevant criminal prosecutions and investigation, and to the supervisors.

**Article 57**
(1) Within 3 months upon entry into force of the present norm, banks shall adopt and implement adequate KYC standards and policies to their own specific activity.
(2) In this respect, during the specified term, banks shall ensure the exiting customers identification and record keeping.

GOVERNOR OF THE NATIONAL BANK OF ROMANIA
MUGUR CONSTANTIN ISARESCU

Bucharest, 26th of February 2002

No. 3

**ANNEX**

Account no. of the client*)

……

……

DECLARATION on real beneficiary identity

The undersigned (client) declare on full responsibility, under law sanctions:

a) that the undersigned is the real beneficiary of the funds/values held into the mentioned account;

b) the real beneficiary/beneficiaries is/are:

Name and Surname/Company Name Address/Premises and Country

……

……

……

The undersigned (client) shall communicate to the bank any change related to the information declared.

Date and place Signature of the client

…… …….

N.B. In case of false declarations or if there are suspicions as regards the reality of information declared, the bank has the right to refuse performing of transactions ordered by the client/to terminate relationships with the client.

*) To be filled in with the name and surname/company name of the client, address/premises.

# GOVERNMENT OF ROMANIA

## Emergency Governmental Ordinance no. 141 /25.10.2001
### on sanctioning certain acts of terrorism and actions of infringement of public order

**Published in the Official Gazette, Part I no. 691 from 31 October 2001**

**The Romanian Government**

On the grounds of provisions of art. 114, par. (4) of the Romanian Constitution,

The Government of Romania has adopted the present Emergency Ordinance.

**Art. 1** – (1) – There are considered acts of terrorism:
a) Offences of murder foreseen by articles 174-176 of the Criminal Code, physical damage and serious physical damage foreseen by art. 181 and art. 182 of the Criminal Code, as well as illegal freedom deprivation foreseen in article 189 of the Criminal Code.
b) Offences foreseen in article 106-109 of Emergency Ordinance no. 29/1997 related to the Aerial Code, republished.
c) Offences of destruction foreseen in art. 217 and art. 218 of the Criminal Code.
d) Offences of disregarding the regime of weapons and munitions, nuclear weapons and other radioactive materials, as well as of explosive materials, foreseen in art. 279 and art. 280 of the Criminal Code, when committed with a view to serious trouble of public order through intimidation, terror or creating a status of panic.

(2) In the event of offences foreseen in par. 1, the maximum of the penalty foreseen by the law is increased by 5 years, without being possible to exceed the general maximum.
(3) Any attempt shall be punished.
(4) It is also considered attempt producing or purchasing the means or instruments, as well taking the measures with a view to comitting the offences foreseen in par. 1.

**Art. 2** – (1) There are considered acts of terrorism and will be punished by prison between 5-20 years and the interdiction of certain rights, the facts of introducing and spreading in the atmosphere, in the soil, in the underground or in water, certain products, substance, materials, micro-organisms or toxins that can endanger the health of humans or animals or the environment, as well as the threats with bombs or other explosive materials, if they are meant to seriously trouble public order through intimidation, terror or through creating a status of panic.
(2) Any attempt is to be punished.

(3) It is also considered attempt producing or purchasing the means or instruments, as well as taking the measures with a view to committing the offences foreseen in par. 1.

**Art. 3** – The agreement with a view to committing terrorist acts will be punished with prison between 3-15 years and the interdiction of certain rights.

**Art. 4** – The threat of a person or a community, by any means, with spreading or using products, substance, materials, micro-organisms or toxins that can endanger the health of humans or animals or the environment is considered crime and will be punished with prison between 6 months – 5 years.

**Art. 5** – The alarming with no grounded reason of a person or of the public, of the specialized bodies in order to intervene in case of danger or of the public order maintenance bodies, by means of correspondence, telephone or any other means of distance communication, which relates to the spreading or use of the products, substance, materials, micro-organisms or toxins foreseen in article 4 will be punished with prison between 3 months – 3 years or with fine.

**Art. 6** – The competence to judge in first instance the crimes foreseen in art. 1 and 2 belongs to the tribunal.
(2) In the event of crimes foreseen in art. 1 and 2, it is mandatory that the criminal pursuit is carried out by the prosecutor.

**Art. 7** – The operators of postal and telecommunication services have the obligation of communicating immediately to the minister of communications and information technology, by written request from the latter, the necessary information with a view to identifying the persons that committed the crimes foreseen in the present emergency ordinance.

**Art. 8** – Disregarding of the obligation foreseen in art. 7 by postal and telecommunication operators is considered contravention and will be sanctioned with fine between ROL 100.000.000 –500.000.000.

PRIME MINISTER
ADRIAN NASTASE

Countersigns:
Minister of Justice, Rodica Mihaela Stanoiu
Minister of Interior, Ioan Rus

Bucharest, 25 October 2001
No. 141