PROGRAMME FINANCED BY THE EUROPEAN UNION UNDER PHARE

EUROPEAN UNION

PHARE PROJECT RO02-IB/JH-08

TRAINING MANUAL ON ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

The Manual has been supervised and edited by Giuseppe Lombardo, Member State Project Leader, and by Massimo Nardo, Manager from UIC, with the assistance of Ms Valeria Roversi (UIC). Contributions came from Nicolae Craiu, (NOPCML Board), Cornel Moldoveanu (NOPCML), Laura Banu (NOPCML), Piero Ricca (UIC)

PRINTED BY C.N. "NATIONAL PRINTING HOUSE"-S.A.

Introduction

This Training Manual revises, updates and expands the earlier document issued in 2002 in connection with Phare Project RO99-IB/JH-02.

In line with the previous document, this is a "Consultation" specialized Training Manual, namely an useful tool to which a wide range of Institutions and officers associated with Anti Money Laundering and Terrorism Financing in Romania may usefully refer to. Therefore, this is not intended to be an Operational Manual, namely a document that "instructs" the user on methodology of training, on curricula etc, because it does not deal with the operations each institution is authorized to conduct by the Romanian legislation on AML and CTF and it does not deal with the procedures each institution applies in the conduct of its business related to ML and TF.

This Training Manual has been complied to help the Public Institutions, Supervision Authorities, Law enforcement agencies etc., people who play an active role on money laundering combat – for running their activities efficiently and effectively and in accordance with the law.

Our goal is to provide some standard policies, procedures and training materials that are designed to help the understanding of criminal activities in the field and take the necessary steps to stop them and limit their effects.

The idea of the first edition of this Manual was to offer a simple, clear tool for the beginners.

We have agreed that the Manual must have a very practical destination, since it will become the source of ready reference in the daily activity of officers and clerks within the institutions it addresses to.

We have therefore devised to include in the Manual the suitable existing materials to give useful information about the main aspects relevant to preventing and combating Money Laundering and Terrorism Financing by screening the materials, which are made available in official sources coming from international institutions and from the organizations who are partners in the Twinning Project. Each source is given explicit acknowledgment.

We consider the Manual as a masterwork of the practitioners offered to practitioners.

Giuseppe Lombardo
Member State Project Leader

Dumitru Cismaru
Member of the NOPCML Board
Representative of the GPO

1. WHAT IS MONEY LAUNDERING?

Sources:

Financial Action Task Force – What is money laundering - Updated Edition, October 2003

Phare Project RO99-IB/JH-02 – Training Manual on Anti Money Laundering – 2002

Phare Project RO02-IB/JH-08 – Suspicious Transaction Guidelines – Updated Edition, Sept 2004

Money laundering is the *de facto* financial side of all criminal offences that generate profit – the activity through which the offender tries to conceal the actual origin and ownership of income derived from criminal activities.

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

The goal of a large number of criminal acts is to generate a profit for the individual or group that carries out the act. Money laundering is the processing of these criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardising their source.

Illegal arms sales, smuggling, and the activities of organized crime, including for example drug trafficking and prostitution rings, can generate huge sums. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits and create the incentive to "legitimise" the ill-gotten gains through money laundering.

When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention.

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.

A) **ML Definition in Romanian Legislation**: 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.

B) **ML Definition in EU Legislation**: Council Directives 91/308/EEC of 10 June 1991 and 2001/97/EC of 4 December 2001:

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

a) or disguising 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 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 indents."

2. MONEY LAUNDERING STAGES

Sources:

Financial Action Task Force – How is money laundered - Updated Edition, October 2003

Phare Project RO99-IB/JH-02 – Training Manual on Anti Money Laundering – 2002

Phare Project RO02-IB/JH-08 – Suspicious Transaction Guidelines – Updated Edition, Sept. 2004

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.

In the initial or placement stage of money laundering, the launderer introduces his illegal profits into the financial system. This might be done by breaking up large amounts of cash into less conspicuous smaller sums that are then deposited directly into a bank account, or by purchasing a series of monetary instruments (cheques, money orders etc.) that are then collected and deposited into accounts at another location.

2. Layering:

After the funds have entered the financial system, the second – or layering – stage takes place.

It is the process of moving money from one account to another in order to disguise their origin.

In this phase, the launderer engages in a series of conversions or movements of the funds to distance them from their source. The funds might be channelled through the purchase and sales of investment instruments, or the launderer might simply wire the funds through a series of accounts at various banks across the globe. This use of widely scattered accounts for laundering is especially prevalent in those jurisdictions that do not co-operate in anti-money laundering investigations. In some instances, the launderer might disguise the transfers as payments for goods or services, thus giving them a legitimate appearance.

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

3. Integration:

Having successfully processed his criminal profits through the first two phases of the money laundering process, the launderer then moves them to the third stage – integration – in which the funds re-enter the legitimate economy. The launderer might choose to invest the funds into real estate, luxury assets, or business ventures.

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.

3. NEED TO COMBAT MONEY LAUNDERING

Sources:

Phare Project RO99-IB/JH-02 – Training Manual on Anti Money Laundering – 2002

Phare Project RO02-IB/JH-08 – Suspicious Transaction Guidelines – Updated Edition, Sept. 2004

FATF - Web Site - Documents

Bucharest International Conference, "Countering Money Laundering and Terrorist Financing: Integrating National Systems in a Consistent "Global Framework" – Bucharest, 14-15 June 2004

The contrast to money laundering has a twofold rationale. On the one hand, combating organized crime and its spreading over the global scenario. On the other hand, sheltering the integrity of financial markets and of market economy.

Combating organized crime

In recent years there has been increasing recognition of the fact that fighting against organized 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 goal of a large number of criminal acts is to generate a profit for the individual or group that carries out the act. Money laundering is the processing of these criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardising their source.

Illegal arms sales, smuggling, and the activities of organized crime, including for example drug trafficking and prostitution rings, can generate huge sums. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits and create the incentive to "legitimise" the ill-gotten gains through money laundering.

When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention.

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 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.

It is normal that money launderers try to move their funds and operations from well regulated countries into offshore centers and emerging economies. Emerging economies not only have weaker or no AML legislation in certain areas, such as the securities or insurance

industries, allowing relatively easy placement of dirty funds, but they usually have high economic growth rates that the money launderers can avail themselves of. Moreover, they are trying hard to attract foreign investments and money launderers can acquire a respectable profile of international investors and even benefit from various economic incentives.

Sheltering the integrity of the market

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.

Domestic business

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

Economies with growing or developing financial centres, but inadequate controls are particularly vulnerable as established financial centre countries implement comprehensive anti-money laundering regimes.

Differences between national anti-money laundering systems will be exploited by launderers, who tend to move their networks to countries and financial systems with weak or ineffective countermeasures.

As with the damaged integrity of an individual financial institution, there is a damping effect on foreign direct investment when a country's commercial and financial sectors are perceived to be subject to the control and influence of organized crime.

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 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.

Reputation

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.

Emerging economies need to protect themselves against money laundering both from domestic and international sources. Combating internal money laundering means fighting against corruption, fraudulent privatization, bank fraud and tax evasion. Combating the placement of international laundered funds helps in protecting domestic businesses and citizens against unfair competition from money launderers and terrorist financing organizations.

Emerging countries also need to avoid being placed on the FATF's list of "non-cooperative jurisdictions" and subject to economic and political sanctions.

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.

A reputation for integrity is the one of the most valuable assets of a financial institution. As the Financial Action Task Force on Money Laundering[1] (FATF) has underlined, if funds from criminal activity can be easily processed through a particular institution – either because its employees or directors have been bribed or because the institution turns a blind eye to the criminal nature of such funds – the institution could be drawn into active complicity with criminals and become part of the criminal network itself: evidence of such complicity will have a damaging effect on the attitudes of other financial intermediaries and of regulatory authorities, as well as ordinary customers.

As for the potential negative macroeconomic consequences of unchecked money laundering the International Monetary Fund has cited inexplicable changes in money demand, prudential risks to bank soundness, contamination effects on legal financial transactions, and increased volatility of international capital flows and exchange rate due to unanticipated cross-border asset transfers.

The expertise gained by the organized 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 imposes its own "rules," which actually means the undermining or even the dissolution of state authority and the rule of Mafia-type arbitrariness.

4. ECONOMIC SYSTEM'S VULNERABILITY TO MONEY LAUNDERING

Sources:

International Monetary Fund: Macroeconomic Implications of Money Laundering - 1996

Phare Project RO99-IB/JH-02 – Training Manual on Anti Money Laundering – 2002

Phare Project RO02-IB/JH-08 – Suspicious Transaction Guidelines – Updated Edition, Sept. 2004

There is no theoretical literature on the macroeconomic effects of money laundering per se. However, some empirical studies coupled with a priori pervasive role of money laundering in criminal and illegal activity, suggest the close relevance of discussion of these

[1] The FAFT is a multi-disciplinary body that brings together the policy-making power of legal, financial and law enforcement experts from its members. It monitors members progress in implementing anti-money laundering measures; reviews and reports on laundering trends, techniques and counter-measures; and promotes the adoption and implementation of FAFT anti-money laundering standards globally.

effects in available studies of the underground economy and crime. However, even taking into account these studies, the discussion is limited and somewhat speculative.

Several studies introduce illegal or underground activity into simple macroeconomic models. Houston (1990) develops a theoretical macro model of business cycle and tax and monetary policy linkages with the underground economy. His investigation of the growth of the underground economy concludes that its effect must be taken into account in setting tax and regulatory policies. More generally, Houston notes that controlling the money supply and forecasting shifts in the price level and interest rates may be made more difficult by the presence of an underground economy that is unobserved. His conclusion is that the presence of significant hidden transactions could lead to overstatement of the inflationary effects of fiscal or monetary stimulus. For example, the increased currency holdings assumed to be induced by money laundering result in reduced inside money expansion. Houston thus sees the growth of crime as possibly contributing to the stagflation phenomenon of the late 1970's and early 1980's.

The common theme of the available research is that if crime, underground activity, and the associated money laundering take place on a sufficiently large scale, then macroeconomic policymakers must take them into account. Failure to do so would result in misdiagnosis and incorrect policy - setting. For example, at the international level, there is little disagreement that the behaviour of monetary aggregates has become in the 1980s and early 1990s more difficult to interpret. This is attributed mainly to the rapid growth of financial technology and economic structures associated with deregulation and privatisation in many countries. However, aggregate growth in money laundering over the same period may also have contributed to the increased volatility of the aggregates, as suggested by the literature. There is the very large size and the timing of some individual criminal activities to consider. Large and irregular individual activities could serve to obscure the economic database and complicate economic policy making. In addition, a key aspect of the understanding of monetary behaviour is being able to identify statistically the country and currency of issuance and the residency of the deposit holder. To the extent that there is a shift in apparent money demand from one economy to another due to cross-border laundering, and the data are thus misleading, this could have consequences for interest and exchange rate volatility, particularly in dollarized economies, as the tracking of monetary aggregates becomes more uncertain.

Income distribution effects of money laundering are not discussed in the literature, but cannot be ignored. To the extent that the underlying criminal activity redirects income from high savers to low savers or from sound investments to risky and lower-quality investments, economic growth will suffer. For example, there is evidence that in the United Sates tax evasion is particularly focused on income derived from the more risky but higher yielding non-corporate capital. Fraud, embezzlement, and insider trading seem likely also to be biased toward more rapidly growing and profitable businesses and markets, because "that's where the money is." Similarly, crimes against the person, such as thefts and kidnappings, seem likely to be directed at wealthier individuals and thus be biased against savings. On the other hand, a drug lord might well have higher propensity to save than a drug user, so that not all distributional effects negatively impact saving and thus economic growth. There is also a particular distributional impact of the money laundering that facilitates tax evasion. Economic costs are compounded in this case because many countries rely on means testing based on declared income for access to a range of government benefits (Tanzi and Shome 1993).

There are indirect macroeconomics effects of money laundering: illegal transactions can deter legal ones by contamination effects. For example, some valid legal transactions by foreigners with Russian entities have been reported to have become less desirable because of

their association with money laundering. More generally, an erosion of confidence in markets, and in the efficiency-signalling role of profits, occurs if there is widespread insider trading, fraud, and embezzlement. Money that is laundered for reasons other than tax evasion represents income that also tends to evade taxes, compounding the economic distortions. There is the contamination bred by contempt for the law, because when one aspect of the law is broken, other financial infringements seem easier to make.

The above discussion relates to money laundering flows. Accumulated balances of laundered assets seem likely to be larger than annual money laundering flow figures. The potential for destabilising and economically inefficient movements, either across borders or domestically, is therefore heightened. The balances accumulated after laundering could be used to corner markets or even smaller economies to the extent that they remain controlled by large-scale organized crime interests. With organized crime contacts, there is further possibility that the control of economic activity can be compounded by insider trading using the balances.

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.

The Financial Action Task Force on Money Laundering has drafted the "Forty Recommendations", which are a comprehensive guidelines for action against money laundering. They cover the criminal justice system and law enforcement, the financial system and its regulation and international co-operation.

In particular Recommendations 10 and 11 impose an obligation on financial institutions to identify their clients. Customer identification in this context means exactly:

Identification of the direct customer – knowing who the person or legal entity is;

Identification of beneficial ownership and control – knowing who ultimately owns or controls the direct customer, and the person on whose behalf a transaction is being conducted;

Verification of the identity of the customer and beneficial owner – corroborating the information provided above;

Due diligence and monitoring - conducting on going checks on the transactions and account throughout the course of the business relationship.

Nevertheless, adequate customer identification procedure could represent a problem in some cases**.**

The more sensitive issue are the ones pertaining to occasional customers; electronic transactions and other cases of lack of a face-to-face identification; the existence of commercial and company laws which allow forms of legal entities in which is possible the anonymity of the shareholders or in which is difficult to disclose the true identity of beneficial owners; the risk of misuse of some types of corporate vehicles and bearer instruments.

At present FATF's efforts are notably aimed at the drafting and diffusion of some principles capable of limiting such a type of corporate vehicles riskiness.

5. ANALYSIS OF MONEY LAUNDERING TECHNIQUES

Sources:

Phare Project RO99-IB/JH-02 – Training Manual on Anti Money Laundering – 2002

Phare Project RO02-IB/JH-08 – Suspicious Transaction Guidelines – Updated Edition, Sept. 2004

Bucharest International Conference, "Countering Money Laundering and Terrorist Financing: Integrating National Systems in a Consistent Global Framework" – Bucharest, 14-15 June 2004

FATF – Annual Reports on Money Laundering Typologies

United Nations Global Programme against Money Laundering – International ML Information Network

It is useful to note some key features that all money launderers seek in constructing their schemes:

- ANONYMITY – making their transactions look normal, so as not to attract attention
- SPEED – rapid movement of assets, to stay ahead of detection

- COMPLEXITY – making the trail hard to follow
- SECRECY – sending assets to places where law enforcement cannot easily follow.

ANONYMITY

It is one of the cardinal rules of money laundering that transactions with criminal assets should be made, as much as possible, to appear like other legitimate transactions in the environment or place where they occur. As a matter of fact cash money does not leave any trail of its origin, besides most of illegal proceeds (deriving from crimes such as drug trafficking, extortion, bribery etc.) usually consist in cash money. In economies where it is quite common to use cash to make both small and large purchases, disposing of cash is not such a great problem for the criminal. However in most countries almost all large transactions are made using other instruments (cheques, bank drafts, credit cards): therefore spending or depositing large amounts of cash gives rise to suspicion. It is for this reason that criminals developed various methods of getting cash into the financial system.

1. Smurfing – breaking large volumes of cash into smaller amounts and having many persons deposit the smaller sums into various bank accounts, or use the sums to purchase other instruments, such as bearer instruments and money orders. Smurfing is primarily used to avoid cash transaction reporting rules that are triggered by a transaction above a certain amount.

2. Cash smuggling – The simple taking of bulk cash out of one country and into another one (generally less strictly regulated) usually by couriers or by hiding it in shipments of goods.

3. Another successful method for getting cash across borders is to use Money remittance systems (see cpt. 7.6)

4. Co-mingling of funds in a cash business. The criminal uses a "legitimate" cash business as a mean to explain the origin of the criminal cash, mixing it with receipts of a shop super markets, petrol stations, restaurants or other enterprises – and depositing the total as the proceeds of the business.

SPEED

Once cash is in the financial system, whether in or out of the country of origin, the launderer can then take advantage of modern money-handling methods to quickly move it around. Electronic banking transfers can move large amounts almost anywhere in the world within few minutes. Movement of funds from one account to another, or across national boundaries, can often be accomplished by the account-holder himself, without having to attend at the bank or involve bank staff.

COMPLEXITY

By putting his funds through a number of transactions, the launderer can make it difficult or impossible for investigators to re-construct the necessary audit trail. Here, multiple wire transfers can be very effective. This consists of electronic transfers of funds from one or several bank accounts to accounts at numerous other financial institutions, usually in different countries. Further transfers can, in turn, be effected from those countries, creating a complex multinational web of transfers that makes it difficult and time-consuming for investigators to follow.

SECRECY

While bank secrecy and financial havens have both a legitimate purpose and a commercial justification, they can also offer unlimited protection to criminals who abuse their intent for the purpose of "doing business at any cost".

Financial havens offer an extensive array of facilities to foreign investors unwilling to disclose the origin of their assets. This includes the registration of international business corporations (IBCs) or shell companies and the services of a number of offshore banks which are not subject to control by regulatory authorities. In many cases, financial havens enforce very strict financial secrecy, effectively shielding foreign investors from investigations and prosecutions in their home country. It is estimated that there are more than 1 million "anonymous" corporations worldwide.

When "dirty" money has sufficiently moved through a "laundry cycle", it is considered cleaned, and made available to the original criminals, with its occupational and geographic origins obscured.

Here follows a list of the techniques more frequently involved.

5.1 - Techniques to Simulate Licit Origin and/ or Dissimulate Illicit Origin

- Laundering in the context of legal business activities controlled by organized crime:
  - over-pricing
  - fake business transactions
  - unregistered acquisition and refinement of raw-materials

  These techniques are used to find a legitimate source to illegal funds: either with the over invoicing of goods which are paid at a lower price or with a totally fake invoice, which could be used to justify an illicit traffic (e.g. drugs). The "black" purchase of raw materials with dirty money allows the criminal to launder it in a following selling

- Loan-back method
  - part of the transferred funds, come back in the shape of a loan. This device, through the capital reimbursement, allows the transfer of ever larger amounts of money.

- Premiums of the insurance polices

- Smurfing

For a better understanding of the techniques used for laundering money, we detailed some of the means that could be used by money-laundering offenders:

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 (smurfing).
- 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 transferred large amounts from a domestic credit institution or from abroad.
- Cash deposits immediately followed by transferring 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 of the loan".

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 clients 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 apparently no commercial activity or where there is no concordance with the commercial activity declared by the client or his background.
- Transfers of the same amounts from the same sender, followed by the cash withdrawals of the transferred amounts.
- Transfers of large amounts, followed by cash withdrawals of the transferred amounts, having the motivation "paying back of the loan".
- Repeated transfers of funds (usually having the same value), through the accounts of involved companies.

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 haven 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 involves numerous bank or travelers 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.

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 havens, having the motivation "buying share company".

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 letterbox 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 offshore company).

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.

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.

- LC's, 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";

5.2 - Techniques to disguise the true ownership

Simple forms of money laundering combine all three stages in one operation like when criminals buy up winning betting slips at a racecourse. This way a "legitimate" receipt is produced and the origin of the funds is concealed in one move. To handle ongoing flows of money criminals need more permanent set-ups like cash based retail services where illegal and legal money are mixed up, and the total sum is reported as legal earnings.

International money laundering involves moving money out of their country of origin either through smuggling or through a front business that appears to have legitimate reasons for sending money abroad. Once abroad, the money can be filtered through financial centres with strict secrecy laws in order to make it virtually untraceable. Finally, the money needs to be made available again. For this many techniques are available. These range from making withdrawals on secure credit cards issued by banks in financial havens to creating bogus capital gains, to setting up front companies that do successful trades with the outside world. The last two types of transactions are made to appear as the result of good business sense but are actually transactions where the launderer is dealing with himself and where his or her foreign company is taking a loss while the domestic company or persona is reaping the rewards.

Money laundering may seem like a technical and remote problem but it is enormous in scope and the underlying crimes are often violent and bloody. Successful money laundering makes the work of law enforcement officials extremely difficult and is thus a threat to the rule of law. It is also a huge problem in sheer volume. An estimate by the then IMF director general Michel Camdessus was that money laundering represented two to five percent of world GDP in 1998, that is between $800 million and $2 trillion per year.

Although money laundering and tax evasion share many techniques and can be run in tandem, the underlying purposes are distinct. In general tax evasion entails taking legally earned income and making it illegal through hiding its origins (transferring it into a less taxable or non-taxable type of income) or hiding it altogether, while money laundering is the reverse process. It takes illegal income and makes it appear legal. Whereas tax evaders underreport their legal earnings thereby paying less tax than they legally should, money launderers often over-report the earnings they make through their legal enterprises thus becoming liable for more tax than they would otherwise be. Tax avoidance, as opposed to tax evasion, is legal, but the policies that invite it may still be classified as "harmful" by the OECD (see below).

According to the OECD, what it terms harmful tax practices distort trade and investment, erode national tax bases and weaken the legitimacy and structure of national tax systems. It has been estimated that developing nations alone lose $50 billion a year due to tax evasion through financial havens.

A bank or another financial institution is engaging in rouge behaviour when it seeks to avoid national and international supervisory, risk-regulating and behavioural standards. The motive for engaging in such behaviour can be to be able to assume the degree of risk these standards seek to prohibit or to achieve freedom of action to engage in illicit activities and market abuse. Under-regulated financial centres increase the potential for regulatory arbitrage. Rogue market actors seek out financial centres with weak supervisory practices, negligible willingness to co-operate and lack of transparency.

Typical instruments through which these techniques are frequently implemented (such as Front men, Corporate vehicles, Offshore destinations, or Nominee and bearer share corporations) are illustrated in cpt. 7.

5.3 - Techniques related to Insurance Sector

Sources:

Phare Project RO99-IB/JH-02 – Training Manual on Anti Money Laundering – 2002

FATF – Annual Reports on Money Laundering Typologies

A number of methods for money laundering in the insurance sector have been detected. At the placement stage of the laundering cycle for example, the industry has been used through the outright purchase of insurance products with criminal cash proceeds. In these cases, money launderers have exploited the fact that insurance products are often sold by brokers–that is, agents who are not acting directly under the control or supervision of the company that issues the product. Thus, the launderer may seek an insurance broker who is not aware of or does not conform to necessary procedures, or else who simply fails to recognise or report information regarding possible cases of money laundering.

There are a number of potential warning signs of possible money laundering, including the potential policy holder being more interested in cancellation terms than the benefits of the policy. The use of cash and/or payment of large single premiums –indeed, the use of large volumes of cash for any payment– should be considered suspicious and as a potential attempt to place criminal funds into the financial system through insurance products.

The receipt of premiums from offshore and/or lightly or unregulated financial intermediaries may also be another sign of potential use of insurance products for laundering purposes. There is an inherent risk both in dealing with and in receiving payments from unregulated intermediaries, as they may often have failed to ensure that thorough due diligence has been conducted on the funds being placed into its policies. It was noted by a number of experts that insurance firms in many jurisdictions often conduct additional due diligence procedures to manage this particular risk.

Another method used for laundering through insurance policies –specifically those used as investment vehicles– is for the launderer to make one or several overpayments of the policy premiums and then request that any reimbursement be paid to a third party. The launderer thus continues to retain the policy as an investment product, while laundering funds through the additional policy contributions/redemptions.

Frequent changes of beneficiaries, using the policy as a bearer asset, or as collateral in part of a wider money laundering scheme together with the early surrender of investment type policies, especially where to do so defies economic logic were also noted as potential money laundering problems by some member countries.

Some of the indicators of potential money laundering mentioned here are relatively easy for a diligent insurer or intermediary to identify. Indeed, in some cases, there may be legitimate reasons for the occurrence of these indicators. However, in a number of the examples provided by the experts in which money laundering had occurred, several indicators were present. It should be noted that many of these indicators appear to be in respect to investment-type life insurance products. As previously mentioned, these instances involve the use of insurance products as a savings or investment vehicle into which dirty money is paid followed by the payment out of some or all the funds in the form of a legitimate appearing redemption.

Other insurance products may be similarly vulnerable to money laundering where there is almost exclusive use of intermediaries (again brokers or agents that are not affiliated with the company that has issued the insurance product). The risk may be even more acute when the relative lack of anti-money laundering requirements or other relevant regulations for this sector is factored in.

5.4 - Preferred Forms of Investment During the Laundering Phase

Before the adoption of the anti-money laundering legislation, organized crime established its legal estates, investing in immovable properties or in industries characterized by presence of small firms, low technology content and generally markets with a certain degree of protection. With the introduction of the penalty of the confiscation of criminal properties, the criminals' preferences already shifted away from immovables, more visible than other kinds of assets. The criminal infiltration of some of the other sectors increased. We do not have strong evidence (though more than rumour has) of criminal infiltration of sectors with large-medium enterprises, high technology, competitive markets. However, in the establishment of the criminal estates, professionals -also well-known professional- were often involved.

After the adoption of the anti-money laundering legislation, criminal propensity to invest in financial assets seems to have increased. Similarly increased it seems to be the market for the intermediation services from the professionals. But in which direction criminals' financial investments are moving is still uncertain.

The evidence we have, actually, does not exclude that organized crime investments could be driven by its professional partners toward legal companies of a certain importance. But it lead us to think that it is difficult to identify the criminal infiltration when the legal entrepreneur is strong enough to avoid the acquisition by the criminals of any kind of control on his firm. In this case criminals – who do not know what trust could be outside their world- should accept what they surely do not like, that is to entrust their legal estates to people they could not control.

Experience shows that the preferred forms of investment carried out during the laundering phase include:

- Financial products[2]:
  - Cash and Banking-Cheques
  - Bonds and Stocks
  - Bank guarantees
  - Primary/ Promissory Bank Guarantees
  - Stand by letter of credit
  - Promissory Notes
- Luxury goods
  - Gold and precious stones
  - Antiques
  - Art Works
- Raw Materials
  - Construction materials
  - Agricultural products

[2] For a more detailed explanation of these techniques please check the Suspicious Transaction Guidelines issued by the National Office for the Prevention and Control of Money Laundering.

Quite often the producers of these products are interested in "black selling" them for tax evasion purposes. Buying them with cash and without any kind of registration the criminals can declare them as "their own products", obtaining in this way the laundering of the dirty money.

5.5. 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.

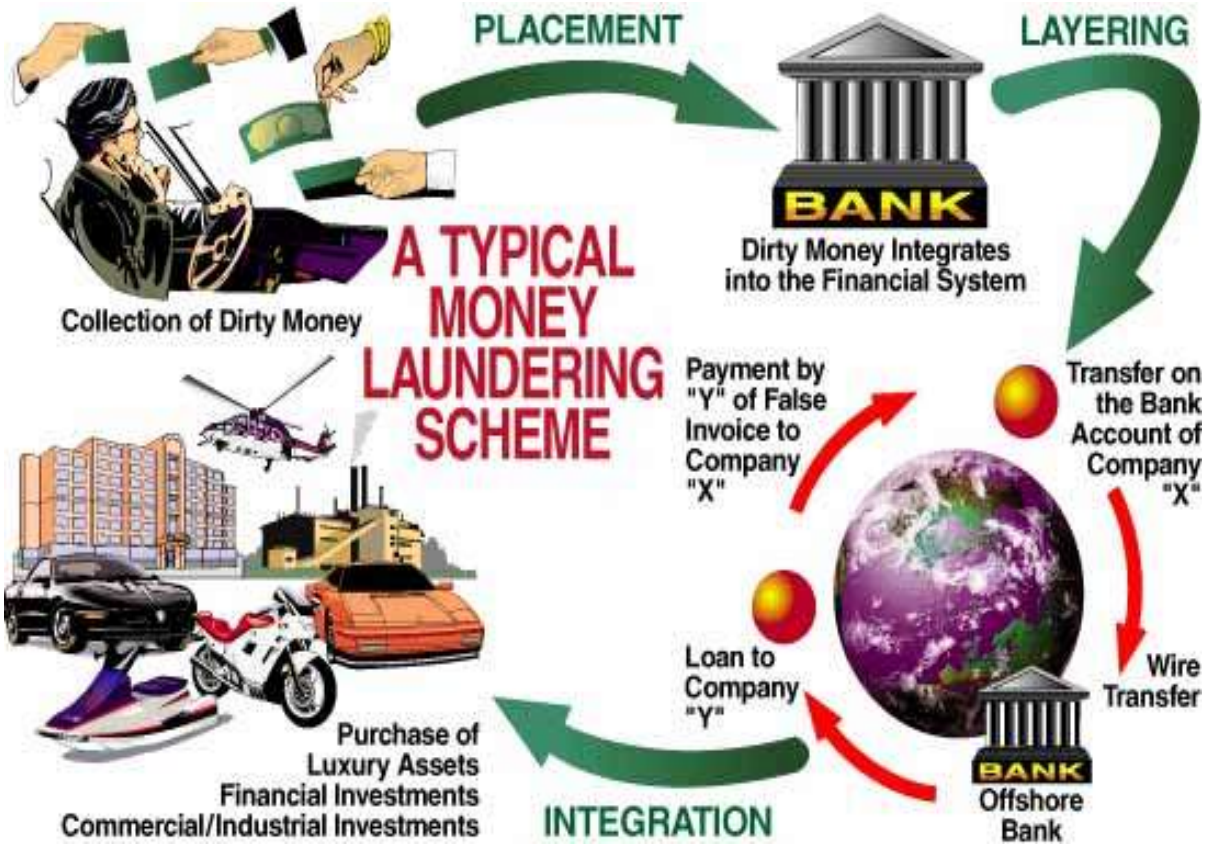
– The client seems to act as agent on behalf of the orderer, whom identity is unknown, and declines, is reluctant or unclear, without having ground reasons, in providing information about that natural or legal person.

– 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.

5.6 - The Money Laundering Cycle (table)

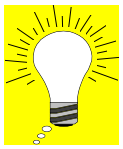


5.7 - Money Laundering Techniques (placement)

PLACEMENT

- **SMUGGLING OF CASH**
- **CONVERSION TO MONETARY INSTRUMENTS/ASSETS**
- **BANK COMPLICITY**
- **"SMURFING"**
- **CO-MINGLE WITH LEGAL FUNDS**
- **MONEY REMITTANCE**
- **INTERNET**
- **CASINOS**

5.8 - Money Laundering Techniques (layering)



LAYERING

NOMINEE OR BEARER CORPS

SELL ASSETS BOUGHT WITH CASH

MULTIPLE WIRE TRANSFERS

OFFSHORE SHELL COMPANIES

5.9 - Money Laundering Techniques (integration)

INTEGRATION

LOAN-BACK SCHEMES

REAL ESTATE PURCHASES

PHANTOM TRADE DEALS

FALSE IMPORT/EXPORT DOCS.

"LEGITIMATE" BUSINESSES

CREDIT CARDS

6. REVIEW OF MONEY LAUNDERING INSTRUMENTS

6.1 Offshore Destinations

Sources:

Phare Project RO99-IB/JH-02 – Training Manual on Anti Money Laundering – 2002

Bucharest International Conference, "Countering Money Laundering and Terrorist Financing: Integrating National Systems in a Consistent Global Framework" – Bucharest, 14-15 June 2004

Once the money has been converted into a form which can be transferred or smuggled, it will often be moved off shore. This has a number of practical advantages. Firstly, it will often in practical terms place the funds beyond the legal reach of the authorities in the jurisdiction where the activity, giving rise to the profits, occurred. Even if the relevant laws are capable of application on an extra-territorial basis, and very few are, by involving another jurisdiction significant practical and financial barriers are placed in the path of investigators in obtaining and securing evidence, which would be admissible before a court. Certain jurisdictions are willing to offer banking and other facilities on the basis that secrecy will be assured. Sadly, there are countries that have been prepared to facilitate the receipt of money no matter what its source. Once the money has been taken offshore it can then enter either directly, or more likely, indirectly into the conventional banking system. Obviously, the more discreet this process is, the better for the launderer. Hence the attraction of jurisdictions that offer either secrecy or in which the level of corruption is sufficient to ensure effective non co-operation with foreign agencies.

Offshore havens are countries and territories, often islands or group of islands, providing freedom from a range of taxes, from exchange controls and offer almost without exception impenetrable bank secrecy and company law benefits.

- Initially predominantly used for tax evasion;
- impenetrable bank secrecy; hardly any cooperation between local authorities (or banks) and institutions (law enforcement and fiscal authorities);
- settlement of transactions usually abroad, formal accounting however offshore;
- in addition to bank secrecy almost complete absence of local taxation and currency exchange controls;
- number of professional advisers supporting the establishment of providing extra services for offshore corporations increasing;
- no activity in the registering country;
- no decision takers in the registering country;
- no liability to pay taxes;
- no proof of the paid-up capital;
- no double taxation agreement;
- no duty to keep books of account;

- excellent infrastructure;
- quick, discrete and low-cost establishment of companies;
- excellent on-site services;
- high demand for offshore entities by criminal individuals/organizations.

In particular, some critical points:

Decision makers: - difficulty to find out the real owner

Usually, the owners of the companies do not have their ordinary residence in the registering country. These persons are represented by nominees. It may happen that even these nominees no longer know who is authorized to take the decisions in such a company (in the core transfer of shares in the company). In such cases, orders are given by means of agreed upon code words.

Books of account

There is no duty to keep books of account – this means that the individual business transactions cannot be reconstructed from the point of view of the criminal police.

Banking secrecy

The strict banking secrecy is to be seen in close connection with the offshore and often cannot be overcome or allows the actual owners of the accounts to transfer money or to develop counter strategies before the accounts have to be disclosed.

Offshore companies should not be accepted as customers, if:

- Registered agents act as directors; beneficial owner obviously prefers anonymity;
- offshore corporation is or pretends to be a holding company; quite often holding structures are set up for the sole purpose of deceiving law enforcement;
- the applicant is offshore trust; advantage is that the owner of assets conveys that ownership to the trust and thus prevents those assets from being seized by creditors. Very popular with money launderers;
- authorized agents apply for the opening of accounts instead of the corporation's managing directors themselves;
- the company is an offshore bank; such shell banks are frequently involved in money laundering and fraud cases.

FATF list of the non-cooperative countries or territories[3]

From the fighting against money laundering viewpoint, FATF identified a list of countries to be considered non co-operative at a rate of:

- Regulation features (existence of types of corporate vehicles that grant anonymity to partners and directors);

[3] July 2004

- banking and financial system (anonymity of accounts and deposits);
- inaccessible bank secrecy;
- control system (deficient or even absent);
- availability to information exchange (usually absent).

    - Cook Islands
    - Indonesia
    - Myanmar
    - Nauru
    - Nigeria
    - Niue
    - Philippines

From the money laundering viewpoint either bank or financial transactions involving these countries may be considered highly risky.

6.1.1 - Tax Havens – A Focus

"Tax havens" means countries, which collect low, taxes and accept fictitious implants of groups which uses these jurisdictions as simple P.O. Boxes. Thus, a group which uses tax havens can make that high transfer prises to be paid for its branch, located in a country with normal taxation system, making more profits in tax havens and lowering them in countries with normal taxation system.

The large interest for the subject represented by the tax haven jurisdictions, linked to the large spreading out of this phenomenon and due to the exotic names of the tax haven countries, should not make us forget that the refuse of paying taxes is not something new (is a negative phenomenon, as old as the existence of tax itself) and the amounts of money which elude the taxes, circulating undisturbed according to the permissive fiscal regulations in this countries, reaches huge level.

The favour benefited by the tax havens is not coming only from the absence of the tax or a low taxation, the non-fiscal advantages offered by those jurisdictions have the same significance.

Nowadays, tax havens represent one of the most common and used procedures for international fraud and evasion.

As some authors consider, the tax havens are the places where money "are laundered whiter that white".

According to other opinions, the tax haven term is "often deceiving and incorrect"; for describing a country from this point of view it should be used the term " the jurisdiction of the financial secrecy".

Almost all countries imposes a certain level of protection for commercial and banking information, but the most of them will not protect these information in case of some inves-

tigations performed by the legal bodies from a foreign country. A jurisdiction of financial and banking secrecy will refuse, almost every time, to infringe his out laws regarding the banking secrecy, even it could be the case of great violation of the law of a country.

Main characteristics of the tax havens:

- Low taxes. In many cases, only some categories of incomes are subject of taxation, with low quotation comparative with the countries of origin of those who appeal to the tax havens; in some countries, no taxes are collected from incomes.
- The secrecy. Most of the countries considered tax havens, ensures the protection of the commercial and banking information.
- Banking activity is getting to play a more important role in the economy of a tax haven than, in the economy of a country, which is not part form, this category. In general, the activity of the foreign citizens is not regulated by strict rules, the taxation in mainly a symbolic one, and the control almost non-existing.
- Promotional publicity. Most tax haven countries make the publicity themselves, including through mediated international conferences, showing the offered fiscal advantages, attracting at this way foreign investors.

Example: Bahamas Islands started a strong campaign to become an elite centre for banking, insurance and ship registering activities.

As far as, the tax is an element of cost for taxable operations, is obvious that the even taxpayers integrate it within the factors, which are determining their strategy.

This attitude can be, ultimately, perfectly legal, as far as it is true that in a "sate of law", the tax payer should estimate the legal framework (it means *fiscal*) he prefers to give his activity; it can't be reproached to him *a priori*, the choice which serves his best interests, as far as the covering laws are permissive.

Looking for the ways with the lowest taxation –which, because it can injure the state interests, find the limit in the theory of abuse of the law– is a process which is facilitated by the existence of tax havens: the tax payer are, really, tempted to obtain profits from advantages offered by many countries or territories which, case by case, are desired or considered otherwise and decrease them, but not evade, the fiscal obligations, in a case or another, to adopt means and ways which can't be injured by the states.

The advantages by which the tax havens are benefiting, are not related only to the low taxation or the absence, which characterises them, but also to the non-fiscal facilities procured by them.

These advantages are strengthened by the communication network – also in the air and maritime transport, and in telephone communication systems, fax, e-mail – and which eliminates the distance and time, considered an element in the banking and financial area.

The tax havens are, the most often, little state who enjoy of political and economical stability which favourite development of financial activity (Panama, Andorra, Liechtenstein, The Virgins Islands, Cayman Islands, Cyprus etc.)

Switzerland is often considered as a tax haven, in a wrong way: the secret bank account has become synonymous with "Switzerland bank account", have another signification then the cases above mentioned. Switzerland is the safest place of money keeping.

The access modalities in a fiscal havens are various, function of the objectives of the taxpayer. There are however two categories:

- **Transfers,** the objective is to minimise the tax value in the countries with fiscal pressure
- **Delocalisation** of tax value can be translated as a suppression of the tax value in origin countries in the advantage of the tax havens.

Transfers

Transfers have the objective to minimise the tax value in the countries with high fiscal pressure. These are made with the occasion of the economic or financial exchange between two taxpayers; one is situated on the territory of a country with a high suppression of the tax value. Because of that, transfers are referred in special to the tax over the company (tax on the profit), indebt be the grand multinational companies.

The proceeding used for producing the searched effect is various: even minimise of the income, even maximise of the deductible task of the same income.

- The transfer made by the proceeding of minimising the income can be obtained by acting on the value of the payment made in benefit of the taxpayer, or to the there date.
- The transfer made by the proceeding of maximising the duties as a result of the application of the symmetric procedures which effects are comparative. The transfer shall be result of the abusive increase of the payments, with the condition to de deductible for calculation of his tax income.

Delocalisation

Comparatively with the transfers, delocalisation can be translated as a suppression of the tax value in origin countries in the advantage of the tax havens. This effect can be obtained in order with the various modalities, which involve, all, the existence of an implanted support in the refugee country.

States cannot stay insensible to the general evasion generated by the existence of tax havens. The fight against transfers and delocalisation are in the attention of the specialised legislation.

The tax havens represent a significant part of the organized crime, been used for money laundering resulted from illegal activities: drug traffic, arms traffic, smuggling etc.

6.2 CORPORATE VEHICLES

Sources:

Oecd - Behind the Corporate Veil. Using Corporate Entities for illicit purposellicit - 2001

Phare Project RO99-IB/JH-02 – Training Manual on Anti Money Laundering – 2002

Corporate vehicles are legal entities through which a wide variety of commercial activities are conducted and assets are held. They are the basis of most commercial and entrepreneurial activities in market-based economies. Corporate vehicles have become an integral and indispensable part of the modern global financial landscape and have contributed immensely to the prosperity and globalisation that have occurred over the last century. Today,

the rapid flows of private capital, ideas, technology, and goods and services involve corporate vehicles at virtually every level.

Despite the important and legitimate roles that corporate vehicles play in the global economic system, these entities may, under certain conditions, be misused for illicit purposes, including money laundering, bribery/corruption, improper insider dealings, illicit tax practices, and other forms for illicit behaviour. Using corporate vehicles as conduits to perpetrate illicit activities is potentially appealing because these vehicles may enable the perpetrators to cloak their malfeasance behind the veil of a separate legal entity. A recent report commissioned by the EC concluded that the ability of legal entities to effectively conceal the identity of their beneficial owners stimulates their use for criminal activities. Even in jurisdictions with bank secrecy laws, perpetrators of illicit activities prefer to deposit their ill-gotten gains in an account opened under the name of a corporate vehicle because bank secrecy protections may be lifted in certain situations.

Any jurisdiction that provides mechanisms enabling individuals to successfully hide their identity behind a corporate vehicle while excessively constraining the capacity of authorities to obtain and share information on beneficial ownership and control for regulatory/supervisory and law enforcement purposes is increasing the vulnerability of its corporate vehicles to misuse. Certain jurisdictions, for example, allow corporate vehicles incorporated or established in their jurisdictions to employ instruments that can be used to obscure beneficial ownership and control, such as bearer shares, nominee shareholders, and nominee directors, without devising effective mechanisms that would enable the authorities to identify the true owners and controllers when illicit activity is suspected or to fulfil their regulatory/supervisory responsibilities. Some of these jurisdictions further protect anonymity by enacting strict secrecy laws that prohibit company registrars, financial institutions, lawyers, accountants, and others, under the threat of civil and criminal sanctions, from disclosing any information regarding beneficial ownership and control to regulatory/supervisory and law enforcement authorities.

Ability to obtain and share information on beneficial ownership and control

In order to effectively combat and prevent the misuse of corporate vehicles for illicit purposes, it is essential that the authorities have the capacity to obtain, on a timely basis, information on the beneficial ownership and control of corporate vehicles. In this Report, *"beneficial ownership"* refers to ultimate beneficial ownership or interest by a natural person. In some situations, uncovering the beneficial owner may involve piercing through various intermediary entities and/or individuals until the true owner who is a natural person is found. With respect to corporations, ownership is held by shareholders or members. In partnership, interests are held by general and limited partners. In trusts and foundations, beneficial ownership refers to beneficiaries, which may also include the settler or founder. In this Report, *"control*" means effective control by an individual or a group of individuals over a corporate vehicle. Thus, with respect to the types of corporate vehicles examined in this Report, the relevant inquiry will be who exercises effective control (rather than legal control) over the corporate vehicle. In many misuses of corporate vehicles, the beneficial owner or settler/founder controls the corporate vehicle despite outward appearances suggesting control by a third party. For example, directors of a corporation could merely be "nominees" who pass on the duties required of a director to the beneficial owner and accept instructions from

the beneficial owner. With respect to trusts, the settler may continue to exercise effective control over the trustee through the use of a trust "protector" and a letter of wishes.

Jurisdictions employ a variety of mechanisms to obtain information on beneficial ownership and control. Most jurisdictions rely on compulsion power, court-issued subpoenas, and other measures to penetrate the legal entity in order to identify the beneficial owner when illicit activity is suspected. In a small number of jurisdictions, the authorities require extensive disclosure of beneficial ownership and control information to the authorities at the formation stage and some impose an obligation to update such information when changes occur. An increasing number of jurisdictions are supplementing these approach by requiring intermediaries involved in the formation and management of corporate vehicles ("corporate service providers") to obtain, verify, and retain records on beneficial ownership and control and to grant authorities access to such records for the purpose of investigating illicit activities, fulfilling their regulatory/supervisory functions, and sharing such information with other authorities domestically and internationally.

The ability of authorities to obtain information on beneficial ownership and control must also be accompanied by corresponding capacity to share that information with other authorities domestically and internationally respecting each jurisdiction's own fundamental legal principles. The ability to share information among domestic authorities, such as securities regulators, law enforcement agencies, banking regulators, and tax authorities is important because certain authorities in a jurisdiction may possess, or have better access to, beneficial ownership and control information that is required by other domestic authorities for regulatory/supervisory or law enforcement purposes. In addition, it is desiderable that the authorities consider ways to make it possible to grant access to beneficial ownerships and control information to agents with authority delegated by the government or the judiciary (such as insolvency administrators) and financial institutions seeking such information in order to comply with customer identification and due diligence ("customer identification") requirements under anti-money laundering laws. The availability of mechanisms to share information domestically also facilitates the efficient use of scarce resources by ensuring that duplicate efforts to obtain beneficial ownership and control information are not undertaken.

Given that anonymity is often enhanced through the use of corporate vehicles incorporated in foreign jurisdictions, it is equally critical that the authorities also have the ability to share information on beneficial ownership and control internationally. Recognising that there are often impediments to effective and efficient exchange of information between jurisdictions, perpetrators often use groups of corporate vehicles, each established in a different high-secrecy jurisdiction, to frustrate any effort by the authorities to identify the beneficial owner.

Several factors affecting the transparency of corporate structures have been identified. There are several cases in which it could be very difficult to ascertain the true identity of the ultimate beneficial owner within legal entities.

In some jurisdictions (the Netherlands, the United Kingdom and many off-shore centers) companies are allowed to act as directors of other companies, for instance. Financial intermediaries find it more convenient to have corporations acting as directors, instead of private individuals, since corporate directorship makes it possible to avoid potential expenses related to the changing of directors whenever staff moves. In addition, this solution could guarantee the coverage of professional indemnity given by insurance policies. Finally,

corporate directors may reduce conflicts of interests that could emerge in cases of groups of companies. Nevertheless, corporate directors may be easier misused because the legal system cannot timely and effectively assign director responsibility to physical persons for illicit corporate behavior. In fact, corporate directors, like nominee directors, can be used to conceal the identity of the beneficial owner and to reduce the level and the quality of the director information reported to the company registry.

Furthermore, a corporate vehicle particularly susceptible to misuse is the International Business Company, which is characterized by non-disclosure of beneficial ownership, anonymity of shareholders through the use of bearer shares, corporate directors and no auditing of accounts.

On these issues, the *OECD Report on Misuse of Corporate Vehicles for Illicit Purposes* has identified some corrective measures to enhance the transparency of the legal entities:

Upfront Disclosure: companies should provide authorities with the information on beneficial ownership and corporate structure at the establishment or incorporation stage;

Intermediary Option: such information should be obtained, verified and kept on record by those intermediaries involved in the establishment and management of corporate vehicles, such as company formation agents, trust companies, lawyers, notaries, trustees, companies supplying nominee shareholders, directors and corporate service providers.

Investigative Mechanism: beneficial ownership and control information is required by authorities only when illicit activity is suspected or when performing their regulatory/supervisory functions.

In these cases two money laundering risks may exist: a) financial assets can be acquired without the purchaser being identified; b) companies may be owned and controlled by people who cannot be identified.

6.3. SHELL COMPANIES

Sources:

FINCEN - The SAR Activity Review. Trends Tips & Issues - Issue 7- august 2004.

Phare Project RO99-IB/JH-02 – Training Manual on Anti Money Laundering – 2002

Bucharest International Conference, "Countering Money Laundering and Terrorist Financing: Integrating National Systems in a Consistent Global Framework" – Bucharest, 14-15 June 2004

FATF – Annual Reports on Money Laundering Typologies

Shell corporations are described as companies with no independent assets or operations of their own, which are used by their owners to conduct business dealings or maintain control of other companies. A shell corporation is registered or licensed in the state or country in which it is incorporated or established, is not traded on a securities exchange, and does not operate on its own. While shell corporations are not illegal or improper, money launderers, tax evaders and terrorist financiers have used shell corporations as a means to disguise the illicit nature of their money. They are easily established and can be interlocked with other shell corporations located all over the world. If a shell corporation is established in

a jurisdiction with strict secrecy laws, it can be almost impossible to identify the owners or directors of the corporation and therefore nearly impossible to trace illicit funds back to their true owner. This is precisely the effect the launderer, terrorist financier and tax evader seeks, and is why shell corporations are an effective means of interrupting the paper trail used by investigators. Shell corporations typically exist only on paper. The corporation's formation documents may list a valid bank account and little more than the name and address of the lawyer or agent handling the incorporation, some officers, and perhaps a few shareholders. When criminals seek to utilize shell corporations to disguise ownership or other illicit activity, they will provide fictitious names or nominee names on the corporate formation documents. These accounts play very important roles in illicit money movements because they can be used to receive deposits and as transfer points to the accounts of other shell corporations, legitimate businesses or individuals. The incorporation documents give shell corporations the outward appearance of legitimate businesses, allowing their bank accounts to be used to receive structured cash deposits designed to avoid currency reporting requirements.

A technique, which has been employed to some effect by criminals and terrorists, is the incorporation of essentially shell companies, which can then "sell" their securities to "overseas investors". The "overseas investors" will be the money laundering puppets. The purchase of such securities, which will be properly documented, will provide a vehicle through which the cleansed money can flow back into the control of those who established the issue. It is important to recognise the use that such companies may be put to in the context of money laundering operations. There have been cases where the existence of operations such as this have been mistaken for high-pressure selling frauds or ‘boiler room' scams. Although the modus operandi may be somewhat similar, especially at the early stages, the purpose and implications of the operation are very different.

The procedures for company formation vary according to the jurisdiction. Company formation agents have thus taken on the role of advising clients on the best locations to establish a legal entity based on his or her individual needs matched to the appropriate jurisdiction. The agent may select a particular jurisdiction because it offers the advantages of rapid formation, low establishment costs, or minimal red tape; or else because it offers "off-the-shelf" companies. He might also choose a location because it does not include information about the owner of a company in public records, or it prohibits altogether the disclosure of such information. He then arranges for the provision of nominee directors and other company officers and registers the company in the optimum location. Increasingly, formation agents also offer other services such as mail/fax receipt and forwarding, telephone answering, administrative services, establishment and administration of bank accounts, or introductory services with particular financial institutions.

A company or legal entity is formed by registering it at a national companies registry. The process varies from jurisdiction to jurisdiction but typically includes designating a director and other officers, selecting a registered office, providing for sale of shares for the company, and filing of appropriate incorporation forms at the registry. Because this process can be complicated and time consuming, individuals desiring to create such an entity have increasingly used the services of specialists in the area – a company formation agent – who performs the administrative task of establishing the company for the individual. The agent may be part of a law or accounting firm or may be a completely independent service.

There is not yet an agreed upon definition for "company formation agent". Based on the information from several experts and the discussions during the exercise itself, a company

formation agent appears to be any agency that assists in the creation of juridical persons or legal entities – specifically "shell companies"– that then may be used for various commercial purposes.

Some of the types of activities seeking the services of a company formation agent might include: import/export trading companies, investment firms, holding companies, consultants, shipping firms, Internet trading firms, and individuals seeking to optimise their fiscal circumstances or protect assets.

6.4. NOMINEE AND BEARER SHARE CORPORATIONS

Sources:

Phare Project RO99-IB/JH-02 – Training Manual on Anti Money Laundering – 2002

FATF – Annual Reports on Money Laundering Typologies

Share certificates are the documents that prove ownership of a corporation. In most countries, the owner of particular shares is registered, and any transfer of those shares to another person must be recorded in a register to be valid. However, some jurisdictions offer the possibility to hold and transfer shares in 'bearer form'. Those bearer shares confer rights of ownership to a company upon the physical holder of the share. In the case of such 'bearer shares' there is no shareholder record, and whoever is in physical possession of the share certificates is the owner. Therefore, it is likely that the true owner of the company does not appear in any company or government records. In the cases in which the identity of the shareholders is not recorded when the share is issued and transferred, ownership of the share is effectively anonymous. Such companies are excellent vehicles for receiving, holding and transferring wealth anonymously.

Information developed shows that bearer securities available in certain jurisdictions represent a particularly useful instrument in the setting up of international money laundering schemes. The bearer cheque is still an important negotiable instrument in use in some regions of the world and could be, along with other types of bearer instruments, another means of laundering criminal proceeds.

Bearer securities

Securities instruments in bearer form consist of bearer bonds and bearer stock certificates or "bearer shares". As with registered securities, both of these instruments are issued by a particular corporate entity in order to raise capital. The difference between registered securities and securities in bearer form, among other things, is the method of transfer. In the case of registered securities, the instrument is issued to a particular individual, and the "owner" is recorded in a register maintained by the issuing entity. In the case of securities in bearer form, the instrument is issued; however, the owner is not recorded in a register. When registered securities are transferred to a new owner, the new owner must be recorded in order for the transfer to be valid. When bearer securities are transferred, since there is no register of owners, the transfer takes place by the physical handing over of the bond or share certificate.

Share certificates, whether in registered or bearer form represent equity within a corporate entity, that is, they represent shareholdings or ownership of a particular corporate entity. The number of shares owned by a person determines the degree of control that such an individual may have over the legal entity that issued the shares. In the case of registered shares, determining ownership is relatively straightforward, as the record of ownership is maintained in the share register of the issuing entity. Determining the ownership of bearer shares, in contrast, is not so easy since it depends on who possesses or has physical control of the share certificates. The obstacles to determining easily the ownership of bearer shares (and thus the ultimate owner of the corporate entity that has issued such instruments) are a factor that has been exploited by launderers to conceal or disguise true ownership of entities used in some money laundering schemes.

A number of FATF member countries have phased out the use of bearer shares and no longer permit corporate entities operating in their territories to issue such instruments. Nevertheless, several FATF members do allow the issue of bearer shares and maintain that they have legitimate functions in facilitating buying and selling of such securities through book entry transfers. They also can be used, according to some sources, for concealing ownership for tax optimisation purposes. In some countries, transparency for law enforcement purposes may be possible by certain other mechanisms or controls. For example, one FATF member indicates that company ownership may be determined through records maintained at company registries. Certain jurisdictions also have rules that require ownership of a listed company to be declared when specified threshold percentages of ownership are reached, and some require bearer shares to be deposited in custodial or safekeeping accounts at financial institutions where anti-money laundering rules on customer identification would normally apply.

Other bearer instruments

When used in the context of money laundering operations, other types of financial instruments in bearer or negotiable form may also be misused. Bearer shares have been used to conceal ownership of corporate vehicles. It is suspected that bearer debt instruments can be used for concealing or disguising the true ownership of funds and for moving them easily without leaving traces that could be picked up by investigators. Bearer or negotiable instruments include certain types of cheques.

Bearer cheques

Bearer cheques are unconditional orders (negotiable instruments) that, when presented to a financial institution, must be paid out to the holder of the instrument rather than to a payee specified on the order itself. Bearer cheques are used in a number of countries. The financial institution is usually not obligated to verify the identity of the presenter of a bearer cheque according to international convention unless the transaction exceeds a particular threshold. A non-bearer cheque may become a bearer instrument, payable to the individual who presents it, when the original payee has endorsed it.

6.5 "GATEKEEPERS"

Sources:

UIC - "Anti Money Laundering Look-out" - Research 1999

FATF – Annual Reports on Money Laundering Typologies

Gatekeepers and money laundering

Experience has often shown financial services professionals and brokers significantly involved in phenomena linked to corporate crime, or in connections between organized crime and legal economy. This has given rise to growing pressures to extend to these professional figures obligations similar to the ones, which anti money laundering legislation had already imposed to more "traditional" players.

Since the core of money laundering is the concealing of the origin of funds, it is easy to suppose that financial professionals and brokers, who set techniques that can reduce the regulatory costs for legal operators, own competencies that can turn out to be particularly useful for criminals to transform illegal profits into legal assets. On the other hand, an agent whose assistance can grant better profits to a legal enterprise or to a prosperous family even at the cost of committing crime, could reasonably have no impediments in obtaining funding from criminals.

Brokerage between legal and criminal economy can be considered as a branch of the wider business brokerage sector, and it is not distinguishable in advance from the other types, but just after discovering the actual crime. Brokerage activity has indeed evolved, specialised and multiplied: especially, financial brokerage has assumed a central role, so as to justify specific policies and tailored institutional answers.

Interposition, indeed, provides a number of advantages.

It usually comes in two main typologies. First, the interposition can be necessary for reasons related to the very nature of the activity in which the intermediation occurs, and to the sector to which the activity belongs. Second, the need for intermediation can arise from the specific features of the relationship between the two principal contracting parties.

Middlemen and wheeler-dealers exist as an answer to the problems, which rise from other people's opportunism. The agent and the broker mark a world in which trust is normal. Middlemen and wheeler-dealers, by contrast, are the product of a world where no trust belongs. In a system where a trusty relationship needs nothing personal to be established (trust being substantially a kind of "public good"), there will be principally agents and brokers. In a set where trust is possible only through selective interpersonal relationships, where interpersonal links and connections are fundamental, agents and brokers will coexist with wheeler-dealers.

The growing difference in the legislation between different countries, mainly in relation with fiscal pressure, has increased the complexity of these activities. Symmetrically, it has increased the opportunities for wheeler-dealers to get into the system, every time it seems expedient to commit irregularities – if not crimes.

Two further reasons consolidate the role of middlemen and wheeler-dealers within business brokerage. First the possibility of taking advantage of more profitable legal systems or of more permissive enforcement modalities —often at the boundary between licit and illicit. Second, the growing intermingling between criminal and legal economy.

Position Advantages

The professional figures we have sketched out so far have usually a high level of expertise in law, economics and accountancy sectors, as well as a lot of experience in negotiating transactions. Moreover, these people have to possess such connections and relations as to guarantee the access to the "right" network in every situation.

This identikit fits perfectly the legal and accountant professionals, because the channels and procedures through which they carry out their activity let them twine close relations whit people other than their clients, such as other professionals involved in similar activities as well as members of private firms and public institutions.

It is easy to suppose that the most favourable position advantages derive from the service of arbitration, which requires a specific knowledge of national and international legal system. The advantages of becoming a business middleman consist in a mix of information and skills in juridical-accounting subjects, so that it is easier to exploit not only national but also international arbitraging opportunities.

Completely different considerations apply to of the business brokerage being carried out in the field of "relational" services where the middleman is expected to get contacts with the best suitable counterparts for the resolution of a problem.

In such a sector the most successful players are those who can exploit a wide network of connections, either for professional or for personal reasons.

Moreover, some elements derived from the public protection granted to these professions can easily be transformed into position advantages; further advantages can come from regulations upon secrecy and privacy regimes, since it is difficult to distinguish between the elements linked to the profession, and thus covered by the secrecy, and the others.

It is easy to understand that these characteristics can become crucial for the choice of a specific person, above all when the intervention of the middleman is justified by the will to conceal the true identity of the principal.

As anti-money laundering measures are implemented in financial institutions, the risk of detection becomes greater for those seeking to use the banking system for laundering criminal proceeds. Increasingly, money launderers seek out the advice or services of specialised professionals to help facilitate their financial operations.

Solicitors, notaries, accountants and other similar professionals perform a number of important functions in helping their clients organize and manage their financial affairs. First of all, they provide advice to individuals and businesses in such matters as investment, company formation,

trusts and other legal arrangements, as well as optimisation of tax situation. Additionally, legal professionals prepare and, as appropriate, file necessary paperwork for the setting up of corporate vehicles or other legal arrangements. Finally, some of these professionals may be directly involved in carrying out specific types of financial transactions (holding or paying out funds relating to the purchase or sale of real estate, for example) on behalf of their clients.

All of these perfectly legitimate functions may also be sought out by organized crime groups or the individual criminal. They may do so for purely economic reasons; however, more important is the desire to profit from the expertise of such professionals in setting up schemes that will help to launder criminal proceeds. This expertise includes both advice on the best corporate vehicles or offshore locations to use for such schemes and the actual establishment of corporations or trusts that make up its framework. Gatekeepers may also be used to offer the veneer of legitimacy to their operations by serving as a sort of intermediary in dealing with financial institutions.

6.6. ALTERNATIVE REMITTANCE SYSTEMS

Sources:

United Kingdom Threat Assessment of Serious and Organized Crime 2003

Phare Project RO99-IB/JH-02 – Training Manual on Anti Money Laundering – 2002

FATF – Annual Reports on Money Laundering Typologies

Alternative remittance (AR) systems enable money to be moved around the world without the use of conventional banking. Alternative remittance can be used for legitimate as well as illegitimate purposes and various forms exist including Hawala banking (the Indian version), Hundi (used by Pakistani communities), Poey Quan (favoured by Thais) and Fie Ch'ien (adopted by Chinese communities). Records are usually kept of all transactions but they may be in dialect, shorthand or a language unfamiliar to law enforce men officers, and could be difficult to interpret.

For obvious reasons, AR banking is attractive to and widely used by serious and organized criminals. It is used not only to launder the proceeds of crime, but to avoid taxes and customs duties. There is also international concern that it may be used in terrorist financing. It is estimated that there are in Europe thousands AR bankers, mostly within Asian communities, where the majority of their customers will be ordinary individuals not criminals. Although discreet in their business dealings, underground bankers are likely to be known within their community and respected for the service they provide in sending monies they earned abroad to families overseas, often at a better exchange rate and lower commission fee than offered by a bank or money services business.

Money transfers are usually used by people without traditional banking relationships, who need to send money to their home country. They can be used by money-launderers too. Through an international network of thousand of agent locations worldwide, people can wire cash quickly (usually within 10 minutes), reliably, conveniently and at attractive prices to recipients in more than 150 countries.

Regional bodies consistently indicate the very significant role that alternative remittance systems appear to play in support of money laundering. Including alternative remittance systems in this year's exercise represents an attempt to provide a clear world-wide focus to the issue.

Although there is not yet a broadly agreed upon definition for "alternative remittance systems", there is some agreement on the common characteristics of such systems. They generally have developed, for example, based on specific ethnic, cultural or historical factors and, in some cases, are a traditional method for moving money that pre-date the spread of Western banking systems in the 19th and 20th centuries. A key factor of such systems – and one that they share with formal or "correspondent" banking – is that value is moved from one location to another often without the physical movement of currency. Alternative remittance systems most frequently operate outside national financial regulatory systems. There are systems, however, that employ elements of the legitimate economy or even of regulated financial services, thus complicating detection by law enforcement authorities. The one consistent element in each alternate remittance system is that all the systems rely upon some form of "netting" or "book transfer" procedure to transmit value.

The experts believed that some of the spread of these systems to new areas is due to immigration, and indeed, such systems often serve as the primary financial service to some immigrant communities. They are secure and less expensive than traditional banks and have sometimes serve as a means to circumvent restrictive currency exchange policies. They also offer a certain amount of anonymity to the user. This last characteristic has given additional incentive for others to make use of alternative remittances systems, including legitimate businesses as well as criminal elements.

6.6.1. General Features.

How can a person pick up a money transfer? The persons may pick up their money transfers at any agent location. The client has to complete a "To Receive Money" form with the following information: name, address, telephone number, amount expected, as well as the sender's name, telephone number, city and state being sent form. Valid identification is also required.

How are money transfers paid out to individual recipients? In most cases, money transfers can be paid out in cash. Some money transfers will be paid out by check, or in a combination of cash and a check. Transactions outside the United States are generally paid in the local currency. However, in some countries transactions are always paid in U.S. Dollars. The recipient may be required to show a valid form of ID. Other restrictions may apply.

How does the system work by using cash? However, the client can only send money by visiting one of the Money Transfer Agents[4] locations and the person has to fill in the "To send money" form with the following information: the name, address, telephone number, the receiver's name, location to be picked up, and the principal dollar amount. The transferred amount and transaction fee is provided to the agent in cash.

[4] *Western Union, for example, is one of the most widespread money remittance networks.*

6.6.2. Hawala/Hundi

Interest in underground banking systems, particularly operative in the Sub-Continent and Middle East has blossomed after the 11th September. While evidence is in part patchy, it is tolerably clear that Al-Qaeda and its associated networks utilised various forms of underground banking to move and store its wealth. What is of particular interest, is the way in which the operations more closely associated with Bin Laden, were able to interface these traditional and informal systems into the conventional financial world, largely through the use of nominee and front companies registered in certain 'off-shore' jurisdictions. It is also clear that religious foundations and even registered charities were utilised not only to collect funds from supporters, but also facilitate integration. Perhaps one of the most disturbing aspects of these revelations was the apparent and pervasive ignorance of law enforcement and intelligence agencies as to the nature, extent and operations of these underground networks. Major intelligence agencies were forced to admit that this was almost an entirely uncharted sea. Perhaps even more disturbingly, recognition is dawning that perhaps these networks cannot be penetrated to the extent necessary to provide the level of intelligence that is required, at least for and proactive action.

The Hawala system originated in southern Asian but has now spread throughout the world following the immigration patterns from that region (to Europe, the Middle East, eastern and southern Africa, North and South America, and other regions of Asia). Hawala is a traditional method form moving funds in south Asia, and its use is known to pre-date the introduction of Western banking practices by hundreds of years.

Despite its prevalence however, hawala operations are illegal in a number of locations. In India, for example, some estimates conclude that up to 50% of the economy uses the hawala system for moving funds, yet it is prohibited by law. Hawala remains a significant method for large number of businesses of all sizes and individuals to repatriate funds and purchase gold. It is also in some cases linked to the movement of narcotics funds as well as transfers associated with smuggling (especially of gold), trafficking in human beings, terrorism, corruption, and customs and excise violations. It is favoured because it usually costs less than moving funds through the banking system, it operates 24 hours per day and every day of the year, it is virtually completely reliable, and there is minimal paperwork required.

The system is based on trust as well as on granted anonymity, since all the operations performed through it leave no paper trail. The users of such a system deliver money across borders without physically moving it. In fact the main feature of Hawala is "compensation" as the people involved are assured the account will be settled by money (or in a number of cases by goods) returned in a future reverse transaction.

With this system, cash is deposited with a "Hawala" dealer (often someone who runs a shop or other small business) who then arranges for an equivalent sum to be collected at a Hawala dealer in another country. The person at the receiving end uses a chit or codeword to prove his entitlement to collect the funds. No actual money moves between the Hawala dealers in each transaction, and there are usually no written records kept of the transactions.

In hawala, funds are moved between individual "hawaladars" which collect funds at one end of the operation and other hawaladars that distribute the funds at the other end. The system is built on a relationship of trust that is not always strictly tied to kinship or other connections. Individual hawaladars usually operate independently of each other rather than as part of a larger organisation. They generally are merchants or small business owners that operate hawala activities alongside their normal business.

As an example, funds which are to be moved from the United Kingdom to India will be provided to a UK hawaladar in UK currency or some other form. This hawaladar then contacts another hawaladar by phone or fax at the destination and requests that an equivalent sum (minus a small percentage charge) be paid out in Indian rupees or gold to the individual designated by the customer in the UK. The process can also move funds in the opposite direction. In instances where accounts become imbalanced between hawaladars over time, the accounts are settled through reciprocal remittances, trade invoice manipulation, gold and precious gem smuggling, the conventional banking system, or by physical movement of currency.

Hawala is considered by those that engage in it as an effective means of moving money. Gold often plays an important role in hawala transactions. Hawala operations are difficult to trace because of the lack of records or, when records exist, the fact that they are somehow coded. The ethnic connection of this system and its strong reliance on trust also make it also difficult to penetrate.

6.6.3. Chinese/East Asian systems

The alternate remittance networks known as the Chinese or East Asian system began in the Far East and, as with hawala, have spread throughout the world following immigration patterns. The system is a traditional one, again as with hawala, predating the introduction of Western banking practices. Originally, it was based on "chits" or tokens – thus it was often referred to as the "Chit system" – today, however, most remitters no longer use chits. The Chinese/East Asian alternative remittance system is used for both legitimate (primarily business and repatriation of emigrant income) and illegal (especially organized crime and narcotics trafficking) money movements.

The entities or agencies offering remittance services take various forms. Often the agent is located in a shop or office and provides the remittance service by itself or in combination with a variety of other services, such as foreign exchange and international fax facilities. Many trading companies and guest houses also operate remittance agencies alongside their main business. Since operating a remittance business requires little more than a fax machine, these agencies are frequently located in residences and operated by a member of the family as a part-time job.

A customer desiring to send money overseas from Hong Kong, for example, must first find a remittance agency that is able to remit money to the overseas destination. Normally a remittance agency will operate in parallel with a sister company or companies overseas. It will then specialise in providing remittance services to the country or countries in which their sister companies are located. To remit money, the customer deposits money into the Hong Kong bank

account of the remittance agent and provides the details of the overseas person or bank account to which the money is to be sent. The remittance agent then contacts its sister company at the destination and instructs it to pay the money to the person or account designated by the customer. If money is sent to Hong Kong, the same process is used in reverse.

Legitimate customers normally use remittance agencies because their service is rapid and inexpensive. Remittance agencies usually charge customers less than banks for international funds transfers. These agencies also generally do not maintain extensive transaction records, require customer identification, conduct background checks on customers, or make reports of suspicious transactions to authorities. Such services are thus very attractive to individuals desiring to conceal the source or destination of their remittances. Persons using remittance agencies for these reasons include international criminals, notably narcotics traffickers, and those wishing to avoid overseas tax and currency regulations.

Remittance agencies make their profit by charging their customers more than the costs incurred in making the remittance. Costs are kept to a minimum when, during a given period, the total amount of money remitted from the agency is roughly the same as the amount remitted to it. In instances where there is a significant imbalance between two sister remittance services, the difference is settled by transferring money using such methods as low cost international transfer services or couriers. Remittance agencies make their money on very narrow profit margins; therefore, the volume of money dealt with must be high for business to be worthwhile.

6.6.4. Other systems

Besides the three major alternate remittance systems focused on during this typologies exercise, a number of FATF members mentioned cases or examples of similar but unrelated systems being used on a smaller scale in their countries. For example, France mentioned what appears to be a remittance network between it and North Africa. Spain also reported detecting such activity between Spain and the Spanish enclave of Melilla in Morocco. Italy cited an example in which representative offices of banks from a Southeast Asian country were providing remittance services to immigrants in Italy from that country. Immigrant populations from Turkey and from the former Yugoslavia also regularly use remittance services to move funds from Germany, and the Netherlands described a system providing this service for its immigrant population from Suriname. Although none of these systems fall into any of the larger schemes, they all share some of the same characteristics: lack of records, customer identification or regulatory oversight, and the potential for misuse by criminals.

6.7.Casinos (and other gambling businesses)

Source:

FATF – Annual Reports on Money Laundering Typologies

Phare Project RO99-IB/JH-02 – Training Manual on Anti Money Laundering – 2002

A casino is a commercial gaming club that provides table games other than bingo, but may also provide other types of gambling e.g. gaming machines (a game of chance machine, which requires coins or tokens to be activated).

Casinos are vulnerable to manipulation by money launderers due to the fast-paced and cash intensive nature of the games and because casinos in a large number of countries provide their customers with a wide array of financial services. Financial services available at casinos are similar and, in many cases, identical to those generally provided by banks and other depository institutions and can include customer deposit or credit accounts, facilities for transmitting and receiving funds transfers directly from other institutions, and cheque cashing and currency exchange services.

Romania casinos do not yet apply "formal" financial services but it may not be excluded that these may be interested in a short future

The experience of law enforcement and regulatory officials suggests that the gambling environment often attracts criminal elements involved in a variety of illicit activities, including fraud, narcotics trafficking and money laundering. With large volumes of currency being brought in and played by legitimate customers, gaming can create a good "cover" for money launderers who are in possession of large amounts of currency. Casinos are also attractive to organized crime if the criminals are able to take over and control the casino, thus providing them with an opportunity to launder their illicit proceeds, as well as engage in other types of criminality. The FATF has consistently noted the use of casinos in money laundering schemes in its annual Typologies Reports, while those countries that require casinos to report suspicious transactions have received significant numbers of STR's.

The money laundering schemes that have been uncovered include instances in which casinos were used by individuals to commit offences including structuring and money laundering, many of them involving organized crime. Also, money launderers have been known to use agents to disguise the true ownership of the funds and are willing to lose some of the money while gambling as a necessary cost of doing business. Other techniques include:

- Buying chips or tokens with cash, conduct minimal betting and then request repayment by a cheque drawn on the casino's account.
- Using a chain of casinos with establishments in different countries and asking for the amount held by the casino in credit for gambler to be made available in another jurisdiction and then withdraw it in the form of a cheque there.
- Asking for winner's cheques to be made out in the name of third persons or without a nominee.

Recent studies of internet gambling suggest that while this form of gambling may still be relatively small, it is growing rapidly. Internet gambling refers to both Internet betting and Internet gaming. Internet betting is making bets using the internet as a conduit to place a bet. The gambling event takes place off-line and the result is independently verifiable i.e. the on-line system does not generate the result, it is used simply for communicating information. The internet is often an alternative to other means of entry to the gambling venue such as the post or telephone. Internet gaming is on-line gaming where the gambling event takes place via the internet and is probably based on a random number generator. The games may appear as virtual-casino style games, slot machine games or interactive lotteries.

The issue of the vulnerability of Internet gambling, which is closely linked to the broader issue of the risks that arise from electronic financial services, is one that the FATF recently considered. The 2001 Typologies Report states: "Internet gambling might be an ideal web-based "service" to serve as a cover for a money laundering scheme through the net.

There is evidence in some FATF jurisdictions that criminals are using the Internet gambling industry to commit crime and to launder the proceeds of crime."

Detection of Suspicious Casino Transactions

In most casinos, officials monitor the gaming activity of customers, usually to ensure that there is proper gambling conduct, rather than as a measure to combat money laundering. However, these officials, together with employees who conduct transactions with a customer are in a unique position to recognise transactions and activities that appear to have no legitimate purpose, are not usual for a specific player or type of players, or are not consistent with transactions involving wagering. This is because while suspicious transactions and activities can take place anywhere in a casino, they usually occur at a casino cage, gaming table or slot machine.

It is not necessary that currency be involved in the transaction for it to be considered suspicious. Sometimes the transactions will be in the form of monetary instruments, wire transfers or credit cards in which the initial placement of illegal proceeds may have occurred at a financial institution or a series of financial institutions. At times customers and/or agents are willing to lose a nominal amount of chips by making small bets or offsetting larger bets and then exchanging the chips for currency, a check or a wire transfer. Suspicious activities often involve structuring to avoid record-keeping or reporting thresholds, using agents to conduct multiple transactions for an anonymous individual, transacting large amounts of funds with little or no related gaming activity (i.e., false drop), providing false documents or identifying information, and layering transactions to disguise their source.

The suspicious nature of the transaction may first be detected by an employee conducting the transaction, a supervisor observing the transaction, or a surveillance department employee monitoring the transaction. In certain instances, there may be facts and circumstances along with the casino's knowledge of its customer, which provide a reasonable explanation for the transaction that would remove it from the suspicious category.

There may be any number of reasons why a transaction, under particular facts and circumstances, is suspicious. In addition, the suspicious nature of transactions is cumulative in its effect. The more frequently any one or combination of these examples occurs at a casino, the more likely it is that the customers conducting these transactions are committing, or may be attempting to commit, financial crimes. The scrutiny needed to identify suspicious transactions highlights the importance of casinos knowing their customers.

A casino must know its customer to make an informed decision as to whether a transaction is suspicious. Many casinos already know a great deal about their customers from information routinely obtained through deposit, credit, cheque cashing and player rating accounts. These accounts generally require casinos to obtain basic identification information about the accountholders and to inquire into the kinds of wagering activities in which the customer is likely to engage. For example, deposit and credit accounts track customer deposits and casino extensions of credit. The player rating account tracks gaming activity and is designed primarily to award complimentary perquisites to volume players, and to serve as a marketing tool to identify frequent customers and to encourage continued patronage. In

certain instances, casinos use credit bureaux to verify information obtained from customers. All of these sources of information can help a casino to understand better its customer base and to evaluate specific transactions that appear to lack justification or otherwise cannot be explained as falling within the usual methods of legitimate business.

The measures currently in place

At a national level, a number of FATF members have required various types of gambling businesses to comply with anti-money laundering obligations, and casinos are generally tightly regulated and supervised, and usually subject to anti-money laundering requirements. In Australia and New Zealand, casinos, gambling houses and bookmakers who open accounts for customers are required to obtain identification before the account can be operated, as well as for all large cash transactions and any suspicious transaction (In New Zealand casinos and gambling houses are the same thing and the "bookmaker" is a government owned and controlled entity). There is also a requirement to report suspicious transactions, and implement other measures to combat money laundering. Similar requirements apply in the United States for casinos and card clubs. In Hong Kong, certain voluntary measures are in place. Customer identification and suspicious transaction reporting obligations apply in Brazil, Iceland and Turkey to lotteries, and in Finland to casinos, horse racing, lotteries and betting agents where the amount of the bet is over 3000 EURO. Portugal has legislation requiring betting and lottery agencies to identify the holders of winning coupons and retain the relevant data for a 10 year period.

The EU Directive now extends to casinos, which are required to identify their customer by means of supporting evidence where gambling chips worth 1000 EURO or more are bought or sold. For casinos subject to state supervision this requirement is deemed to be complied with if their customers are registered and identified on entry to the casino. Where money laundering is suspected, the casino must identify the customer regardless of the amount involved, and is also obliged to file an STR with the competent authority. They are obliged to implement internal control measures and train their staff concerning money laundering issues.

In most jurisdictions, casinos and some other gaming entities are subject to some type of licensing or registration, regulation and supervision because of their vulnerability to various forms of criminal activity including money laundering, illegal betting, race or game fixing etc. However governments have regulated such businesses for other reasons as well, such as the need to ensure that gamblers receive fair treatment when gambling, and to protect persons that are potentially vulnerable. In certain jurisdictions, casinos are indirectly owned by the government, while in others private ownership is allowed, but usually on the basis of fairly strict licensing requirements. Where there is private ownership, a tight regulatory regime is intended to protect customers and ensure that the casino does not fall within the ownership or control of criminals or their associates. In addition, there are usually extensive checks on casino owners and operators. In some jurisdictions, casinos and certain other gambling entities have fit and proper tests for senior management, screening programmes for senior staff, and various compliance and training programmes.

6.8 USE OF THE INTERNET

Sources:

Phare Project RO99-IB/JH-02 – Training Manual on Anti Money Laundering – 2002

FATF – Annual Reports on Money Laundering Typologies

Finansinspektionen - Reports

General issues

During the past year, the number of financial institutions offering on-line banking facilities has continued to grow. A lot of banks and financial institutions are offering their services "on-line". The range of services available also appears to be growing – along with the acceptance and usage of electronic payment systems by the general public. However, these trends vary from one jurisdiction to another.

The account below presents only an overview of the various types of services currently offered consumers via the Internet.

Banks

The following Internet services are offered by banks that provide their customers with services via the Internet.

Accounts: Customer may go in and check their balances in various accounts in the bank. Certain banks also offer the possibility to open accounts via the Internet.

Payment services: Customers can make transfers between accounts and pay bills.

E-invoices and e-giro are the designations for two different ways of handling invoices.

E-commerce: Certain big banks have begun to develop e-commerce sites by linking up corporate and private customers. In such cases, the banks offer corporate and private customers the possibility to establish contact and order the products of the bank's corporate customers.

Loans: Customers can download application documents from the bank's web pages. Some banks also offer the possibility to apply for loans through the Internet. However, an agreement is not concluded until the customer manually signs the debt instrument.

Securities trading: Customers are offered the possibility to sell and buy mutual fund units. Some banks also offer the possibility to conclude agreements concerning fund custodial accounts through the Internet and provide share price information. Customers can buy and sell shares through the Internet. Some banks also offer the possibility of concluding agreements covering share custodial accounts through the Internet.

Information: Customers gain access to highly extensive information. In addition to information concerning the bank's products and services, several banks also provide information concerning share prices, index trends and so forth.

Advice: The term advice is not unambiguous. As a guide, however, the act prohibiting professional advice in certain cases defines advisory services as operations "in which professional experts offer advice or other assistance to others in legal or financial matters". In the survey responses, several banks state that they provide advice, although the extent of this varies. Some banks state that they provide general private advice in financial questions while others almost exclusively focus their advice on market and corporate analyses in the securities area.

In the bank sector, traditional customer contacts via branch offices and postal services continue to dominate. The capacity of the office network, however, is limited and the possibility to service several customers simultaneously is considerably larger via the telephone and Internet. Individual smaller banks already use the Internet as their dominant customer channel.

Securities Companies

The Internet-based operations of securities companies are, of course, focused on trading in securities. A number of other services such as lending, payment services and various types of information are linked to this.

Securities trading: Via Web-linked securities companies, customers can trade shares and other securities such as options, warrants and convertibles. The companies also offer their customers the possibility to sell and buy mutual fund units.

Advice: Only one of the respondent companies in the survey stated that it provided advisory services via the Net.

Share price information: Share price information is frequently somewhat outdated when shown on the screen.

Analyses: The companies usually provide their own analyses and those of others. It should also be noted that certain banks and securities companies provide mobile services via wireless application protocol (WAP) and SMS. Although these services are available for use, the suppliers of the necessary technical support in the form of, for instance, mobile telephones have not provided the products in large numbers.

It is worth to underline that, in some of the countries classified as non co-operative (namely Nauru), it is possible to obtain a license for the incorporation of banks tailored to operate exclusively through telematic networks. The opening of bank correspondence accounts with other banks based themselves in countries lacking of a suitable regulation allows, as a matter of fact, to transfer funds towards other destinations (such a device is being widely used by the Russian economic crime).

The risk of money laundering is therefore very high due to the fact that the Internet offers easy and almost universal access, eliminates face-to-face contact and is extremely fast and effectively eliminates borders.

There are three characteristics of the Internet that together tend to aggravate certain "conventional" money laundering risks:

- the ease of access through the Internet,
- the depersonalisation of contact between the customer and the institution, and
- the rapidity of electronic transactions.

Although these factors could be considered as contributing positively to the level of efficiency and the reduction of costs of financial services, they also make customer identification and routine monitoring of accounts and transactions by financial institutions more difficult.

A potential risk exists at any first stage of the contact between a new customer and a financial institution. The financial institution must deal with certain difficulties which are essentially the same regardless of the type of account. It must verify the identity of a natural

person, who may, for example, present false or forged documentation. It must establish adequate identification of legal entities when determination cannot be made of the legal existence or nature of the business. It must also verify the signature authority for any account that is opened when it is not clear whether the customer is acting on his own behalf. In the case of Internet banking, the difficulties for the financial institution are increased if the procedures for opening such an account are permitted to take place without face to face contact or without a link to an already existing traditional account.

Once the initial identification of the customer has been accomplished, it is usually assumed by the financial institution that it is the identified customer who continues to perform transactions on the account. This assumption is probably a valid one for traditional bank accounts. However, if an account is accessed through the Internet, there is no human intervention that might help to detect suspicious or unusual activity, such as instances in which individuals other than the account holder perform transactions on the account. Information on access to the account from other geographic locations – another possible indicator of unusual activity – would also not necessarily be detectable.

Furthermore, account managers may be responsible for too many accounts and therefore less able to monitor activities of individual account holders – even if ultimately equipped with monitoring software.

FATF members have identified a possible method of money laundering through the Internet. The scheme would involve the launderer establishing a company which offered services that were payable through the Internet. The launderer would then use, or in fact pretend to use, those Internet services, charging them to his credit or debit cards that were linked to his offshore bank account (the account containing his criminal proceeds). His company then invoices the credit card company, which, in turn, forwards the payment for the service rendered.

In this example, the credit card company, Internet service provider, Internet invoicing service and even the bank would likely have no reason to believe there was anything suspicious about the activity, since they each only see one part of it. Such schemes would be extremely hard to detect, at least through the traditional means of suspicious transaction reporting.

Jurisdictional issues

Determining jurisdiction for the licensing and supervision of financial services offered through the Internet remains a concern for the FATF. Financial regulatory agencies may not be able to ensure that financial services available through the Internet within their national jurisdictions (but from servers outside the jurisdiction) follow adequate anti-money laundering procedures. From the investigative perspective, jurisdictional issues arise in determining where an on-line transaction has taken place in order to know where investigative authorities should go to seek documentary evidence of transactions linked to money laundering activity.

All information conveyed through the Internet passes through a series of computer servers. Each connection from a particular server should leave traces (i.e., a record of its IP number, date and time of connection etc.) on those servers with which it communicates. This

information is only available, however, if the receiving servers at each step have been set up to create "log files". If the log files exist at each step and the user sending the information has a fixed IP address, it is relatively straightforward to trace back from the addressee to the originator. In instances where the user is operating using dial-up access, his or her identity can be discovered through the log files of the ISP.

However, if the log files are not maintained at any step of the way, or dial-up user (or subscriber) information is considered to be protected information, then it may be more difficult to determine the ultimate link between an illegal activity and a specific individual.

Internet gambling

It seems that Internet gambling might be an ideal web-based "service" to serve as a cover for a money laundering scheme through the net. There is evidence that criminals are using the Internet gambling industry to commit crime and to launder the proceeds of crime. Despite attempts to deal with the potential problems of Internet gambling by regulating it, requiring licenses in order to operate, or banning such services outright, a number of concerns remain in addition to the inability to track the Internet links mentioned above. For example, transactions are primarily performed through credit cards, and the offshore placement of many Internet gambling sites makes locating and prosecuting the relevant parties more difficult if not impossible. Furthermore, gambling transactions, the records of which might be needed as evidence, are conducted at the gambling site and are software-based; this may add to the difficulty of collecting and presenting such evidence.

7. MONEY LAUNDERING AND FINANCING OF TERRORISM

Sources:

Phare Project RO99-IB/JH-02 – Training Manual on Anti Money Laundering – 2002

FATF Documents: Freezing terrorist Asstes: International Best Practices – 3.10.2003; Combating the abuse of alternative remittance systems: International Best Practices – 20.06.2003; Combating the abuse of non profit organisations: International Best Practices – 11.10.2002

7.1 THE PHENOMENON OF FINANCING OF TERRORISM

The primary objective of terrorism according to one definition is "to intimidate a population, or to compel a Government of an international organisation to do or abstain from doing any act"[5] In contrast, financial gain is generally the objective of other types of criminal activities. While the difference in ultimate goals between each of these activities may be true to some extent, terrorist organisations still require financial support in order to achieve their aims. A successful terrorist group, like any criminal organisation, is therefore necessarily one that is able to build and maintain an effective financial infrastructure. Experts generally believe that terrorist

[5] Article 2, International Convention for the Suppression of the Financing of Terrorism, 9 December 1999.

financing comes from two primary sources. The first source is the financial support provided by States or organisations with large enough infrastructures to collect and then make funds available to the terrorist organisation. This so-called State-sponsored terrorism has declined in recent years, according to some experts, and is increasingly replaced by other types of backing. An individual with sufficient financial means may also provide substantial funding to terrorist groups. Osama bin Laden, for example, is thought to have contributed significant amounts of his personal fortune to the establishment and support of the Al-Qaeda terrorist network. 12. The second major source of funds for terrorist organisations is income derived directly from various "revenue-generating" activities. As with criminal organisations, a terrorist group's income may be derived from crime or other unlawful activities.

After the terrorist attacks in New York, it emerged a new need to combine efforts and experience in the war against terrorist financing. This allowed to see more clearly the mosaic of terrorist financing and the movement of suspected terrorist funds. Terrorist groups differ from other criminal organizations because of the object behind the crime. In fact, unlike organized crime groups, that primarily seek monetary gain, terrorist groups usually have "non-financial goals" but dissemination of an ideology or more simply, just showing intimidation. In spite of this, due to the undeniable necessity to "transfer" sources of financing, the experience gained in the field by financial intelligence units, revealed itself as the most effective instrument to discover and block terrorist-related assets.

7.2 RELATIONSHIPS BETWEEN MONEY LAUNDERING AND FINANCING OF TERRORISM

Terrorist financing is different from classic money laundering. In cases of money laundering, the proceeds of illicit activity are laundered or layered in ways to make the proceeds appear legitimate, and the ultimate goal is usually the attainment of more money. With terrorist financing, the source of funding or financing is often "legitimate" and the ultimate goal is not necessarily the attainment of more funds.

Community solicitation and fundraising appeals are one very effective means of raising funds to support terrorism. Often such fundraising is carried out in the name of organisations having the status of a charitable or relief organisation, and it may be targeted at a particular community. Some members of the community are led to believe that they are giving for a good cause. In many cases, the charities to which donations are given are in fact legitimate in that they do engage in some of the

From a technical perspective, the methods used by terrorists and their associates to generate funds from illegal sources differ little from those used by traditional criminal organisations. Although it would seem logical that funding from legitimate sources would not need to be laundered, there is nevertheless often a need for the terrorist group to obscure or disguise links between it and its legitimate funding sources. It follows then that terrorist groups must similarly find ways to launder these funds in order to be able to use them without drawing the attention of authorities. In examining terrorist related financial activity, FATF experts have concluded that terrorists and their support organisations generally use the same methods as criminal groups to launder funds. Some of the particular methods detected with

respect to various terrorist groups include: cash smuggling (both by couriers or bulk cash shipments), structured deposits to or withdrawals from bank accounts, purchases of various types of monetary instruments (travellers' cheques, bank cheques, money orders), use of credit or debit cards, and wire transfers.

The difference between legally and illegally obtained proceeds raises an important legal problem as far as applying anti-money laundering measures to terrorist financing. Money laundering has generally been defined as a process whereby funds obtained through or generated by criminal activity are moved or concealed in order to obscure the link between the crime and generated funds. The terrorist's ultimate aim on the other hand is not to generate profit from his fundraising

When terrorists or terrorist organisations obtain their financial support from legal sources (donations, sales of publications etc.), there are certain factors that make detecting and tracing these funds more difficult. For example, charities or non-profit organisations and other legal entities have been cited as playing an important role in the financing of some terrorist groups. The apparent legal source of this funding may mean that there are few, if any, indicators that would make an individual financial transaction or series of transactions stand out as linked to terrorist activities.

Other important aspects of terrorist financing that make its detection more difficult are the size and nature of the transactions involved. Several FATF experts have mentioned that the funding needed to mount a terrorist attack does not always call for large sums of money, and the associated transactions are usually not complex. For example, an examination of the financial connections among the September 11th hijackers showed that most of the individual transactions were small sums, that is, below the usual cash transaction reporting thresholds, and in most cases the operations consisted of only wire transfers. The individuals were ostensibly foreign students who appeared to be receiving money from their parents or in the form of grants for their studies, thus the transactions would not have been identified as needing additional scrutiny by the financial institutions involved.

Nevertheless, there are similarities in the way international organized crime and terrorist organizations move money or attempt to hide their financial tracks. International terrorist groups need money to attract, support, and retain adherents throughout the world as well as to secure the loyalty of other groups that share the same goals. Thus, there is a need to devise schemes to raise, collect, and distribute money to operatives preparing for attacks. Therefore, this "need to move money" makes the terrorist funds particularly vulnerable to detection and financial intelligence, which is crucial in combating terrorist financing.

7.3 MAIN SOURCES OF TERRORIST FUNDING

Experts generally believe that terrorist financing comes from two primary sources. The first source is the financial support provided by States or organisations with large enough infrastructures to collect and then make funds available to the terrorist organisation. This so-called State-sponsored terrorism has declined in recent years, according to some experts, and is increasingly replaced by other types of backing. An individual with sufficient financial means may also provide substantial funding to terrorist groups. Osama bin Laden, for example, is thought to have contributed significant amounts of his personal fortune to the establishment and support of the Al-Qaeda terrorist network.

The second major source of funds for terrorist organisations is income derived directly from various "revenue-generating" activities. As with criminal organisations, a terrorist group's income may be derived from crime or other unlawful activities.

To give an overview on the main sources of funding and the means used to move money that terrorist organisations use to support their networks, it is possible to underline that persons investigated for terrorist activity have carried out operations through the money remittance network operating worldwide. Very often funds have been transferred abroad through those informal money transfer networks collecting the remittances of foreign citizens belonging to specific nationalities who live in several countries involved in the fight against terrorism, for such entities, operating through the banking system, have developed their activity internationally.

In other cases, natural persons made cash payments in different countries, for quite high amounts and in favour of the same account. After that funds so collected were transferred towards Asia or the US. With this respect it is worth that the names of the payee partially coincided with the names included in one of the lists mentioned below.

But the most common instrument, especially Al-Qaida uses in order to support its terrorist groups is an "informal system of moving money", the so-called "Hawala" system, mentioned before.

7.4 THE NEW FATF RECOMMENDATIONS ON FINANCING OF TERRORISM

The FATF held a special session in Washington on October 29, 2001 and decided to expand its mandate to include the fight against terrorist financing. The group adopted eight recommendations for blocking terrorist organizations to obtain and transfer funds for their criminal activities. Such recommendations will represent the new international standard in the fight against terrorist financing. The agreement on the Special Recommendations commits FATF members to:

- Take immediate steps to ratify and implement the relevant United Nations instruments.
- Criminalise the financing of terrorism, terrorist acts and terrorist organisations.
- Freeze and confiscate terrorist assets.
- Report suspicious transactions linked to terrorism.
- Provide the widest possible range of assistance to other countries' law enforcement and regulatory authorities for terrorist financing investigations.

- Impose anti-money laundering requirements on alternative remittance systems.
- Strengthen customer identification measures in international and domestic wire transfers.
- Ensure that entities, in particular non-profit organisations, cannot be misused to finance terrorism

Last but not least, FATF has extended to all over the world its invitation to take part in this process on the same terms of FATF members, emphasizing the importance of "global" cooperation in this field.

An additional Recommendation, "Special Recommendation IX", regarding cash courriers, was adopted on October 22 2004.

7.5. BEST PRACTICES DEVELOPED BY FATF

FATF has indicated a set of "best practises" related to freezing of terrorist assets, combating the abuse of alternative remittance systems, and the abuse of non profit organizations.

7.5.1. Freezing of terrorist assets

1) Establishing effective regimes and competent authorities or courts.

According to FATF Jurisdictions should establish the necessary legal authority and procedures, and designate accountable, competent authorities or courts responsible for:

a) freezing the funds or other assets of designated persons;

b) lifting such freezing action;

c) providing access to frozen funds or other assets in certain circumstances. Jurisdictions may undertake the following best practices to establish a comprehensive and effective terrorist financing freezing regime:

(i) Develop a designation process which authorises a competent authority or a court to freeze funds or other assets based on information creating reasonable grounds, or a reasonable basis, to suspect or believe that such funds or other assets are terrorist-related. Jurisdictions may adopt executive, administrative or judicial procedures in this regard, provided that:

a) a competent authority or a court is immediately available to determine whether reasonable grounds, or a reasonable basis, to suspect or believe that a person or entity is a terrorist, terrorist organisation or associated person or entity exits;

b) terrorist-related funds or other assets are frozen immediately upon a determination that such reasonable grounds, or a reasonable basis, to suspect or believe exists; and

c) freezing occurs without prior notice to the parties whose funds or other assets are being frozen. These procedures may complement existing civil and/or criminal seizure and forfeiture laws, and other available judicial procedures;

(ii) Establish effective procedures to facilitate communication, co-operation and collaboration among relevant governmental agencies and entities, as appropriate, during the designation process in order to:

a) develop all available information to accurately identify designated persons (e.g. birth date, address, citizenship or passport number for individuals; locations, date and jurisdiction of incorporation, partnership or association for entities etc.) and

b) consider and co-ordinate, as appropriate, any designation with other options and actions for addressing terrorists, terrorist organisations and associated persons and entities;

(iii) Develop a process for financial institutions to communicate information concerning frozen funds or other assets (name, accounts, amounts) to the competent authorities or courts in their jurisdiction. Identify, assess the impact of, and amend, as necessary and to the extent possible, existing bank secrecy provisions or data protection rules that may prohibit this communication to appropriate authorities of information concerning frozen terrorist-related funds or other assets;

(iv) Identify and accommodate the concerns of the intelligence community, law enforcement, private sector and legal systems arising from circulation of sensitive information concerning frozen terrorist-related funds or other assets;

(v) Develop a publicly known delisting process for considering any new arguments or evidence that may negate the basis for freezing funds or other assets6 and develop procedures for reviewing the appropriateness of a freezing action upon presentation of any such new information;

(vi) Develop procedures to ensure that adequate prohibitions against the publication of sensitive information exist in accordance with applicable legislation;

(vii) Develop procedures and designate competent authorities or courts responsible for providing access to frozen funds or other assets in accordance with S/RES/1452(2002) to mitigate, where appropriate and feasible, unintended consequences of freezing action; and

(viii) Consider enacting hold-harmless or public indemnity7 laws to shield financial institutions, their personnel, government officials, and other appropriate persons from legal liability when acting in good faith according to applicable law to implement the requirements of a terrorist financing freezing regime.

2) Facilitating communication and co-operation with foreign governments and international institutions.

To the extent legally and constitutionally possible, according to FATF jurisdictions may undertake the following best practices to improve international co-operation and the effectiveness of the international campaign against terrorist financing by sharing information relating to the freezing of terrorist-related funds or other assets:

(i) Develop a system for mutual, early, and rapid pre-notification of pending designations, through diplomatic and other appropriate channels, where security concerns and applicable legal principles permit, to those jurisdictions invited to join in a designation and/or where funds or other assets of designated persons might be located, so that funds or other assets can be frozen simultaneously across jurisdictions with the objective of preventing terrorists, terrorist organisations and associated persons and entities from hiding or moving them. In this regard, consideration should be given to establishing a list of relevant contacts to ensure that freezing action is taken rapidly;

(ii) Develop a system for undertaking useful and appropriate consultation with other jurisdictions for the purpose of gathering, verifying, and correcting identifier information for designated persons as well as, where appropriate and where intelligence concerns and applicable laws permit, the sharing and development of information on possible terrorists and terrorist financing activity of the parties involved. In undertaking such consultation, jurisdictions should consider:

a) the greater effectiveness of freezing on the basis of accurate and complete identifying information;

b) the burden created by unsubstantiated or incomplete identifying information;

c) the security concerns associated with releasing sensitive identifier or corroborating information; and

d) the degree of danger or urgency associated with the potential designated persons. Where appropriate such information should be shared and developed before a designation is made;

(iii) Prepare a packet of information for each potential designation that includes as much information as is available and appropriate to identify the designated person accurately and to set forth the basis for the potential designation in any pre-notification or communication of the designation;

(iv) Develop a process for rapidly and globally communicating new designations and the accompanying packet of information to other jurisdictions;

(v) Share on a mutual and confidential basis, to the extent possible, with other jurisdictions information about the amount of funds or other assets frozen pursuant to terrorist financing freezing orders by account;

3) Facilitating communication with the private sector.

Because terrorist-related funds or other assets overwhelmingly are held in the private sector, FATF recommends jurisdictions to develop efficient and effective means of communicating terrorist financing-related information with the general public, particularly financial institutions. To the extent possible and practicable, jurisdictions can adopt the following practices to develop and enhance communication with the private sector regarding the freezing of terrorist-related funds or other assets, the availability of additional information concerning existing designations, and other counter-terrorist financing guidance or instruction:

(i) Integrate, organize, publish and update without delay the designated persons list, for example both alphabetically and by date of designation to assist financial institutions in freezing terrorist-related funds or other assets and making the list as user-friendly as possible. Create different entries for different aliases or different spellings of names. Where technologically possible provide a consolidated list in an electronic format with a clear indication of changes and additions.;

(ii) Develop clear guidance to the private sector, particularly financial institutions, with respect to their obligations in freezing terrorist-related funds or other assets;

(iii) Identify all financial institutions for use in notification and regulatory oversight and enforcement of freezing action related to terrorist financing, utilising, where appropriate and feasible, existing registration or licensing information;

(iv) Develop appropriate regulatory authorities and procedures where applicable, and properly identify a point of contact to assist financial institutions in freezing terrorist-related funds or other assets and to address, where feasible, unforeseen or unintended consequences resulting from freezing action (such as the handling and disposition of perishable or wasting funds or other assets and authorising access to funds or other assets in accordance with S/RES/1452(2002)); and

(v) Elaborate clear guidance to the private sector with respect to any permitted transactions in administering frozen funds or other assets (e.g. bank charges, fees, interest payments, crediting on frozen accounts etc).

4) Ensuring adequate compliance, controls, and reporting in the private sector.

Jurisdictions may work with the private sector in developing the following practices to:

a) facilitate co-operation and compliance by the private sector in identifying and freezing funds or other assets of designated persons, and

b) prevent designated persons from conducting financial or other transactions within their territories or through their financial institutions:

(vi) Co-operate with the private sector generally and financial institutions in particular, especially those that are independently implementing programs to prevent potential terrorist financing activity or those that have come forward with potentially incriminating information, in investigating possible financial activity by a designated person;

(vii) Ensure that financial institutions develop and maintain adequate internal controls (including due diligence procedures and training programs as appropriate) to identify the existing accounts, transactions, funds or other assets of designated persons;

(viii) Ensure that financial institutions immediately freeze any identified funds or other assets held or controlled by designated persons;

(ix) Ensure that financial institutions implement reasonable procedures to prevent designated persons from conducting transactions with, in or through them;

(x) Develop an effective monitoring system by a competent authority or a court with sufficient supervisory experience, authority and resources

(xi) Identify, assess compliance with, and improve as necessary client or customer identification rules used by financial institutions;

(xii) Identify, assess compliance with, and improve as necessary record keeping requirements of financial institutions;

(xiii) Adopt reasonable measures to consider beneficial owners, signatories and power of attorney with respect to accounts or transactions held by financial institutions when searching for activity by designated persons, including any ongoing business relationships;

5) Ensuring thorough follow-up investigation, co-ordination with law enforcement, intelligence and security authorities, and appropriate feedback to the private sector.

Financial information pertaining to designated persons is extremely valuable to law enforcement and other security authorities investigating terrorist financing networks. Law enforcement and prosecutorial authorities should, therefore, be given access to such information.

Jurisdictions may adopt the following practices to ensure that information available from the private sector in freezing terrorist related funds or other assets is fully exploited:

(i) Develop procedures to ensure that appropriate intelligence and law enforcement bodies and authorities receive, share, and act on information gathered from the private sector's freezing of terrorist-related funds or other assets, including sharing such information internationally to the extent possible and appropriate;

(ii) Develop procedures to ensure that, to the extent possible and appropriate, law enforcement authorities provide feedback to financial institutions indicating how financial intelligence is being used to support law enforcement actions.

7.5.2. Combating the abuse of alternative remittance systems

In addition to their use by legitimate clients, criminals have laundered the proceeds of various criminal activities using Money and other Values Transfer (MVT) services. Primarily, unregulated MVT services permit funds to be sent anonymously, allowing the money launderer or terrorist financier to freely send funds without having to identify himself or herself. In some cases, few or no records are kept. In other cases, records may be kept, but are inaccessible to authorities. The lack of adequate records makes it extremely difficult, if not impossible, to trace the funds after the transaction has been completed.

Analysis of the investigations and law-enforcement activities of various jurisdictions indicate several ways in which informal MVT services have been abused by terrorists and launderers and suggests areas in which preventive measures should be considered.

(i) Licensing/Registration

A core element of Special Recommendation VI is that jurisdictions should require licensing or registration of persons (natural or legal) that provide informal MVT services. The FATF defines these terms in its interpretative note to Special Recommendation VI. A key element of both registration and licensing is the requirement that the relevant regulatory body is aware of the existence of the business. The key difference between the two is that licensing implies that the regulatory body has inspected and sanctioned the particular operator to conduct such a business whereas registration means that the operator has been entered into the regulator's list of operators.

a. Requirement to Register or License

At a minimum, jurisdictions should ensure that MVT services are required to register with a designated competent authority such as a Financial Intelligence Unit (FIU) or financial sector regulatory body. Registration of MVT services is likely to be a relatively cost effective approach when compared to the significant resources required for licensing.

The obligation of licensing or registration applies to agents. At a minimum, the principal business must maintain a current list of agents, which must be made available to the designated competent authority. An agent is any person who provides MVT service under the direction of or by contract with a legally registered or licensed MVT service (for example, licensees, franchisees, concessionaires.

b. Applications for Licence

In determining whether an application for licensing can be accepted by the regulatory authority, it is clear that some form of scrutiny of the application and the operator needs to be conducted.

Authorities should conduct background checks on the operators, owners, directors and shareholders of MVT services. When considering the suitability of a potential operator, the authorities should conduct a criminal record check on the principal persons having control over the operations of the MVT service, as well as consult appropriate law enforcement databases, including suspicious or unusual reporting filings. Consideration should be given to defining the type of criminal record which would make the applicant ineligible to operate a licensed MVT service.

c. Business Address

MVT services should be required to submit details of the addresses from which they operate and to notify the authorities upon any change of address or cessation of business. Where possible, this information may be made available to both the public so they may check which MVT service is properly licensed or registered before using their services, and to investigative/regulatory authorities during the course of their work. This also has value for financial institutions with which the MVT services maintain accounts as they are able to identify which MVT services are licensed/registered and thus are more able to identify illegal operators and to report to the FIU or appropriate competent authority accordingly.

d. Accounts

In processing cash and in the settlement of transactions, MVT services use bank accounts. Some operators run a number of businesses, of which MVT service is one, and use business accounts to conduct or conceal the remittances of funds on behalf of their clients thereby masking the true origin of the commingled funds and accounts. VT services should maintain the name and address of any depository institution with which the operator maintains a transaction account for the purpose of the MVT service business. These accounts must be capable of being identified and should be held in the name of the registered/licensed entity so that the accounts and the register or list of licensed entities can be easily cross-referenced.

Traditional financial institutions should be encouraged to develop more detailed understanding as to how MVT services utilise bank accounts to conduct their operations, particularly when accounts are used in the settlement process.

(ii) Identification and Awareness Raising

Some informal MVT services are not known to regulatory and enforcement agencies, which makes them attractive to the financiers of terrorism. Identification of these MVT services will make it less attractive for criminal and terrorist groups to use them to facilitate and hide the financing of their activities.

For the majority of jurisdictions, proactive identification of informal MVT services is an integral element of establishing and maintaining an effective registration/licensing regime. Once informal MVT services have been located, compliance programs can be instituted under which the agents are approached, their details are recorded and they are provided information as to their obligations. Once regulatory regimes are in place, ongoing compliance work will include strategies to identify those MVT services not yet known to regulatory authorities.

Jurisdictions may apply a range of strategies to uncover MVT services, using a number of approaches concurrently. Jurisdictions are encouraged to foster close co-ordination within the relevant authorities for the purposes of developing inter-agency strategies and using available resources to identify MVT services that may be operating illegally. Below is a list of suggested best practices for identifying MVT services and raising public awareness about their activities. As best practices, it is recognized that some of these suggestions may not be appropriate for every jurisdiction and that each jurisdiction must develop strategies best suited to its individual system.

a. Identification Strategies

Best practices in the area of identification strategies include: Examining the full range of media to detect advertising conducted by informal MVT services and informing operators of their registration/licensing obligations. This includes national, local and community newspapers, radio and the Internet; giving particular attention to the printed media in various communities; and monitoring activities in certain neighbourhoods or areas where informal MVT services may be operating.

During investigations, information about informal MVT services may be uncovered which should be passed on to the competent authorities. Best practices include encouraging investigators to pay particular attention to ledgers of business that may be associated with informal MVT services; encouraging enforcement agencies to look for patterns of activity that might indicate involvement of informal MVT services; and, where possible, encouraging enforcement agencies to consider using undercover techniques or other specific investigative techniques to detect MVT services that may be operating illegally. Consulting with the operators of registered/licensed MVT services for potential leads on MVT services that are unregistered or unlicensed.

Being aware that informal MVT services are often utilised where there is bulk currency moved internationally, particularly when couriers are involved. Paying particular attention to the origin and owners of any such currency. Couriers could provide insights for the identification and potential prosecution of illegal operators with whom the couriers are associated, especially when potential violations by couriers are linked back to the source of the informal MVT service operation.

Paying particular attention to domestic suspicious transaction or unusual activity reporting, as well as to domestic and international large value cash reporting, to identify possible links to informal MVT services.

Assisting banks and other financial institutions in developing an understanding of what activities/indicators are suggestive of informal MVT service operations and using this to identify them. Many informal MVT services maintain bank accounts and conduct transactions in the formal financial sector as part of other business operations. Giving banks the authority to crosscheck particular accounts against a register of these operators and notify the relevant regulatory authority as appropriate.

Once informal MVT services are identified international exchange of information and intelligence on these entities between the relevant bodies can be facilitated. Consideration could be given to sharing domestic registers with international counterparts. This strategy would also assist jurisdictions to identify local operators not previously known.

b. Awareness Raising Campaigns

Best practices in the area of awareness raising campaigns include:

Making informal MVT services aware of their obligations to license or register, as well as any other obligations with which they may have to comply. Ensuring that the competent authorities responsible for overseeing and/or registering or licensing informal MVT services know how to detect those services that have not registered or been licensed. Finally, ensuring that law enforcement is aware of the compliance requirements for MVT services in addition to the methods by which those services are used for illicit purposes.

Using education and compliance programs, including visits to businesses which may be operating informal MVT services to advise them of licensing or registration and reporting obligations, as opportunities to seek information about others in their industry. Using these outreach efforts by law enforcement and regulatory agencies to enhance their understanding about the operations, record-keeping functions and customer bases of informal MVT services.

Extending outreach campaigns to businesses typically servicing informal MVT services (such as shipping services, courier services and trading companies). Placing in trade journals, newspapers or other publications of general distribution notices of the need for informal MVT services to register or license and file reports.

Ensuring that the full range of training, awareness opportunities and other forms of education are provided to investigators with information about MVT services, their obligations under the regulatory regime and ways in which their services can be used by money launderers and terrorist financiers. This information can be provided through training courses, presentations at seminars and conferences, articles in policing journals and other publications.

Issuing various financial sector publications of guidelines to encourage licensing or registration and reporting and also general material to ensure financial institutions currently subject to suspicious transaction reporting requirements develop an understanding of MVT services. (Also see section on suspicious transaction reporting on page 9.) Informing potential customers about the risks of utilizing illegal MVT services and their role in financing of terrorism and money laundering.

Requiring entities to display their registration/license to customers once they are registered/licensed. Legitimate clients will likely have a higher degree of confidence in using registered/licensed operators and may therefore seek out those operators displaying such documentation.

Making a list of all licensed or registered persons that provide MVT services publicly available.

(iii) Anti-Money Laundering Regulations

The second element of Special Recommendation VI is that jurisdictions should ensure MVT services are subject to FATF Recommendations 4-16 and 21-25 and also to the Eight Special Recommendations.

There is key information that both regulatory and enforcement bodies need access to if they are to conduct effective investigations of money laundering and terrorist financing involving MVT services. Essentially, agencies need the information about the customers, the transactions themselves, any suspicious transactions, the MVT service's location and the accounts used. The MVT service must also have further records on hand available to regulatory and enforcement bodies as needed.

It is considered that to be effective in addressing the problem of MVT services, regulations should not be overly restrictive. Regulation must allow for those who abuse these systems to be found and stopped, but it should not be so burdensome that it in effect causes

the systems to go "underground", making it even harder to uncover money laundering and terrorist financing through alternative remittance.

(iv) Compliance Monitoring

Regulatory authorities need to monitor the sector with a view to identifying illegal operators and use of these facilities by criminal and terrorist groups. Jurisdictions are encouraged to consider the following options:

Competent authorities should also be entitled to check on unregistered entities that are suspected to be involved in MVT services. There should be an effective process for using this authority.

Granting regulatory agencies or supervisory authorities the authority to check the operations of a MVT service and make unexpected visits to operators to allow for the checking of the register's details and the inspection of records. Record keeping practices should be given particular attention.

Establishing a process of identifying and classifying operators which are considered to be of high risk. In this context, "high risk" means those operators which are considered to be of high risk of being used to carry out money laundering or terrorist financing activities. Jurisdictions are encouraged to give such high risk entities extra attention from supervising authorities.

(v) Sanctions

In designing legislation to address this problem, one of the aspects to be considered concerns the sanctions which are available to redress non-compliance. If a MVT service operator is found to be non-compliant with the relevant requirements of the legislation the competent authorities would be expected to sanction the operator. Ideally, jurisdictions should set up a system to employ civil, criminal or administrative sanctions depending on the severity of the offence. For instance, in some cases a warning may initially suffice. However, if a MVT service continues to be in non-compliance, it should receive stronger measures. There should be particularly strong penalties for MVT services and their operators that knowingly act against the law, for example by not registering.

To monitor the continued suitability of an individual to conduct a MVT service, jurisdictions are encouraged to put systems into place which would bring any conviction of an operator, shareholder or director following licensing or registration, to the attention of the appropriate authorities. Consideration should be given to defining the type of criminal record which would make the applicant ineligible to be a MVT service provider.

7.5.3. Misuse of non profit organisations

The misuse of non-profit organisations for the financing of terrorism is coming to be recognised as a crucial weak point in the global struggle to stop such funding at its source. This issue has captured the attention of the Financial Action Task Force (FATF), the G7, and the United Nations, as well as national authorities in many regions. Within the FATF, this has rightly become the priority focus of work to implement Special Recommendation VIII (Non-profit organisations).

Non-profit organisations can take on a variety of forms, depending on the jurisdiction and legal system. Within FATF members, law and practice recognise associations, founda-

tions, fundraising committees, community service organisations, corporations of public interest, limited companies, Public Benevolent Institutions, all as legitimate forms of non-profit organisation, just to name a few.

This variety of legal forms, as well as the adoption of a risk-based approach to the problem, militates in favour of a functional, rather than a legalistic definition. Accordingly, the FATF has developed suggested practices that would best aid authorities to protect non-profit organisations that engage in raising or disbursing funds for charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works" from being misused or exploited by the financiers of terrorism.

According to FATF the following principles guide the establishment of these best practices: Government oversight should be flexible, effective, and proportional to the risk of abuse.

Mechanisms that reduce the compliance burden without creating loopholes for terrorist financiers should be given due consideration. Small organisations that do not raise significant amounts of money from public sources, and locally based associations or organisations whose primary function is to redistribute resources among members may not necessarily require enhanced government oversight.

Different jurisdictions approach the regulation of non-profit organisations from different constitutional, legal, regulatory, and institutional frameworks, and any international standards or range of models must allow for such differences, while adhering to the goals of establishing transparency and accountability in the ways in which non-profit organisations collect and transmit funds. It is understood as well that jurisdictions may be restricted in their ability to regulate religious activity.

Jurisdictions may differ on the scope of purposes and activities that are within the definition of "charity," but all should agree that it does not include activities that directly or indirectly support terrorism, including actions that could serve to induce or compensate for participation in terrorist acts.

The non-profit sector in many jurisdictions has representational, self-regulatory, watchdog, and accreditation organisations that can and should play a role in the protection of the sector against abuse, in the context of a public-private partnership. Measures to strengthen self-regulation should be encouraged as a significant method of decreasing the risk of misuse by terrorist groups.

Preliminary analysis of the investigations, blocking actions, and law-enforcement activities of various jurisdictions indicate several ways in which non-profit organisations have been misused by terrorists and suggests areas in which preventive measures should be considered.

(i) Financial transparency

Non-profit organisations collect hundreds of billions of dollars annually from donors and distribute those monies – after paying for their own administrative costs – to benficiaries.

Transparency is in the interest of the donors, organisations, and authorities. However, the sheer volume of transactions conducted by non-profit organisations combined with the desire not to unduly burden legitimate organisations generally underscore the importance of risk and size-based proportionality in setting the appropriate level of rules and oversight in this area.

a. Financial accounting

Non-profit organisations should maintain and be able to present full program budgets that account for all programme expenses. These budgets should indicate the identity of

recipients and how the money is to be used. The administrative budget should also be protected from diversion through similar oversight, reporting, and safeguards.

Independent auditing is a widely recognised method of ensuring that that accounts of an organisation accurately reflect the reality of its finances and should be considered a best practice.

Many major non-profit organisations undergo audits to retain donor confidence, and regulatory authorities in some jurisdictions require them for non-profit organisations. Where practical, such audits should be conducted to ensure that such organisations are not being abused by terrorist groups. It should be noted that such financial auditing is not a guarantee that program funds are actually reaching the intended beneficiaries.

b. Bank accounts:

It is considered a best practice for non-profit organisations that handle funds to maintain registered bank accounts, keep its funds in them, and utilise formal or registered financial channels for transferring funds, especially overseas. Where feasible, therefore, non-profit organisations that handle large amounts of money should use formal financial systems to conduct their financial transactions. Adoption of this best practice would bring the accounts of non-profit organisations, by and large, within the formal banking system and under the relevant controls or regulations of that system.

(ii) Programmatic verification

The need to verify adequately the activities of a non-profit organisation is critical. In several instances, programmes that were reported to the home office were not being implemented as represented. The funds were in fact being diverted to terrorist organisations. Non-profit organisations should be in a position to know and to verify that funds have been spent as advertised and planned.

a. Solicitations

Solicitations for donations should accurately and transparently tell donors the purpose(s) for which donations are being collected. The non-profit organisation should then ensure that such funds are used for the purpose stated.

b. Oversight

To help ensure that funds are reaching the intended beneficiary, non-profit organisations should ask following general questions:

- Have projects actually been carried out?
- Are the beneficiaries real?
- Have the intended beneficiaries received the funds that were sent for them?
- Are all funds, assets, and premises accounted for?

c. Field examinations

In several instances, financial accounting and auditing might be insufficient protection against the abuse of non-profit organisations. Direct field audits of programmes may be, in some instances, the only method for detecting misdirection of funds. Examination of field operations is clearly a superior mechanism for discovering malfeasance of all kinds, including

diversion of funds to terrorists. Given considerations of risk-based proportionality, across-the-board examination of all programmes would not be required. However, non-profit organisations should track programme accomplishments as well as finances. Where warranted, examinations to verify reports should be conducted.

d. Foreign operations

When the home office of the non-profit organisation is in one country and the beneficent operations take place in another, the competent authorities of both jurisdictions should strive to exchange information and co-ordinate oversight or investigative work, in accordance with their comparative advantages. Where possible, a non-profit organisation should take appropriate measures to account for funds and services delivered in locations other than in its home jurisdiction.

(iii) Administration

Non-profit organisations should be able to document their administrative, managerial, and policy control over their operations. The role of the Board of Directors, or its equivalent, is key.

Much has been written about the responsibilities of Boards of Directors in the corporate world and recent years have seen an increased focus and scrutiny of the important role of the Directors in the healthy and ethical functioning of the corporation. Directors of non-profit organisations, or those with equivalent responsibility for the direction and control of an organisation's management, likewise have a responsibility to act with due diligence and a concern that the organisation operates ethically. The directors or those exercising ultimate control over a non-profit organisation need to know who is acting in the organisation's name – in particular, responsible parties such as office directors, plenipotentiaries, those with signing authority and fiduciaries. Directors should exercise care, taking proactive verification measures whenever feasible, to ensure their partner organisations and those to which they provide funding, services, or material support, are not being penetrated or manipulated by terrorists.

Directors should act with diligence and probity in carrying out their duties. Lack of knowledge or passive involvement in the organisation's affairs does not absolve a director – or one who controls the activities or budget of a non-profit organisation – of responsibility. To this end, directors have responsibilities to:

The organisation and its members to ensure the financial health of the organisation and that it focuses on its stated mandate.

Those with whom the organisation interacts, like donors, clients, suppliers.

All levels of government that in any way regulate the organisation.

These responsibilities take on new meaning in light of the potential abuse of non-for-profit organisations for terrorist financing. If a non-profit organisation has a board of directors, the board of directors should:

Be able to identify positively each board and executive member;

Meet on a regular basis, keep records of the decisions taken at these meetings and through these meetings;

Formalise the manner in which elections to the board are conducted as well as the manner in which a director can be removed;

Ensure that there is an annual independent review of the finances and accounts of the organisation;

Ensure that there are appropriate financial controls over program spending, including programs undertaken through agreements with other organisations;

Ensure an appropriate balance between spending on direct programme delivery and administration;

Ensure that procedures are put in place to prevent the use of the organisation's facilities or assets to support or condone terrorist activities.

Oversight bodies

Various bodies in different jurisdictions interact with the charitable community. In general, preventing misuse of non-profit organisations or fundraising organisations by terrorists has not been a historical focus of their work. Rather, the thrust of oversight, regulation, and accreditation to date has been maintaining donor confidence through combating waste and fraud, as well as ensuring that government tax relief benefits, where applicable, go to appropriate organisations. While much of this oversight focus is fairly easily transferable to the fight against terrorist finance, this will also require a broadening of focus.

There is not a single correct approach to ensuring appropriate transparency within non-profit organisations, and different jurisdictions use different methods to achieve this end. In some, independent charity commissions have an oversight role, in other jurisdictions government ministries are directly involved, just to take two examples. Tax authorities play a role in some jurisdictions, but not in others. Other authorities that have roles to play in the fight against terrorist finance include law enforcement agencies and bank regulators. Far from all the bodies are governmental – private sector watchdog or accreditation organisations play an important role in many jurisdictions.

(i) Government Law Enforcement and Security officials

Non-profit organisations funding terrorism are operating illegally, just like any other illicit financier; therefore, much of the fight against the abuse of non-profit organisations will continue torely heavily on law enforcement and security officials. Non-profit organisations are not exempt from the criminal laws that apply to individuals or business enterprises.

Law enforcement and security officials should continue to play a key role in the combat against the abuse of non-profit organisations by terrorist groups, including by continuing their ongoing activities with regard to non-profit organisations

(ii) Specialised Government Regulatory Bodies

A brief overview of the pattern of specialised government regulation of non-profit organisations shows a great variety of practice. In England and Wales, such regulation is housed in a special Charities Commission. In the United States, any specialised government regulation occurs at the sub-national (state) level. GCC member countries oversee non-profit organisations with a variety of regulatory bodies, including government ministerial and intergovernmental agencies.

In all cases, there should be interagency outreach and discussion within governments on the issue of terrorist financing – especially between those agencies that have traditionally dealt with terrorism and regulatory bodies that may not be aware of the terrorist financing risk to non-profit organisations. Specifically, terrorist financing experts should work with non-

profit organisation oversight authorities to raise awareness of the problem, and they should alert these authorities to the specific characteristics of terrorist financing.

(iii) Government Bank, Tax, and Financial Regulatory Authorities

While bank regulators are not usually engaged in the oversight of non-profit organisations, the earlier discussion of the importance of requiring charitable fund-raising and transfer of funds to go through formal or registered channels underscores the benefit of enlisting the established powers of the bank regulatory system – suspicious activity reporting, know-your-customer (KYC) rules etc – in the fight against terrorist abuse or exploitation of non-profit organisations.

In those jurisdictions that provide tax benefits to charities, tax authorities have a high level of interaction with the charitable community. This expertise is of special importance to the fight against terrorist finance, since it tends to focus on the financial workings of charities.

Jurisdictions which collect financial information on charities for the purposes of tax deductions should encourage the sharing of such information with government bodies involved in the combating of terrorism (including FIU's) to the maximum extent possible. Though such tax related information may be sensitive, authorities should ensure that information relevant to the misuse of non-profit organisations by terrorist groups or supporters is shared as appropriate.

(iv) Private Sector Watchdog Organisations

In the countries and jurisdictions where they exist, the private sector watchdog or accreditation organisations are a unique resource that should be a focal point of international efforts to combat the abuse of non-profit organisations by terrorists. Not only do they contain observers knowledgeable of fundraising organisations, they are also very directly interested in preserving the legitimacy and reputation of the non-profit organisations. More than any other class of participants, they have long been engaged in the development and promulgation of "best practices" for these organisations in a wide array of functions.

Jurisdictions should make every effort to reach out and engage such watchdog and accreditation organisations in their attempt to put best practices into place for combating the misuse of non-profit organisations. Such engagement could include a dialogue on how to improve such practices.

Sanctions

Countries should use existing laws and regulations or establish any such new laws or regulations to establish effective and proportionate administrative, civil, or criminal penalties for those who misuse charities for terrorist financing.

7.6. THE LISTS OF SUSPECTED TERRORISTS

Since September 11th, a number of lists, annexed to the Regulations of the European Council, which impose the freezing of all assets of natural and legal persons connected to the Talibans and to some terrorist organisations, circulated among all countries engaged in the fight against this crime.

7.6.1. Public lists

Additionally to the lists alleged to the Regulations of the European Union several lists have been released on account to the indications provided by the Basle Committee of Banking Supervisors, US Treasury Office for Foreign Assets Control (OFAC), US Federal Bureau of Investigation (FBI), US FIU (FINCEN).

7.6.2. Non Public lists

In a number of countries, investigating judges have involved the national FIU in the analysis of the financial implications several cases have given rise to, with the purpose of ascertaining whether business relations established within the local financial sector could be connected to persons and entities being investigated. It is to be underlined that judges have in most cases authorised the relevant Financial Intelligence Unit to disclose the list of natural and legal persons involved in judicial proceedings to foreign FIU's. While within each country the lists in hand have been circulated usually among financial institutions through the national financial sector associations.

7.6.3. A third kind of lists

In the case of persons or entities not belonging to any list, in several countries they have been grouped in the so called category of individuals and legal persons "reported as possibly connected to terrorist activities". In such a framework the reasons for reporting may depend on various elements. The most common examples are the following: personal data of the persons being reported partially coincide with names included in the lists, the persons/entities being reported appear to be in business relations with those listed; persons/entities reported to be connected to terrorist activities by the media.

8. EXAMPLES OF ROMANIAN AND OTHER COUNTRIES' EXPERIENCE

Case 1: Corruption Infractions

Source: NOPCML

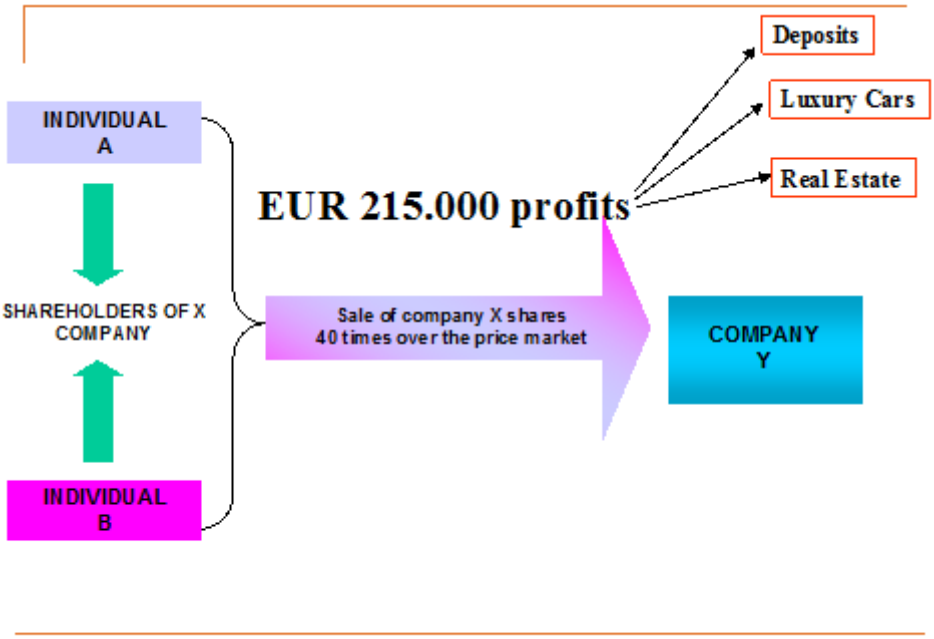
Individuals A and B have sold to the Company Y stock of shares of Company X. The transaction has been concluded at a price 40 times bigger than the market price. After a few days, the two individuals have acquired the same number of shares, but this time at the market price, 40 times inferior to the price of the suspicious transaction. Therefore, the two individuals have managed to keep the initial position of shareholders of Company X, registering a staggering total profit of EUR 215,000.

The two individuals worked at the time as public functionaries with a State Institution.

It has been proven that the exceptional profit achieved by the two above mentioned individuals (EUR 215,000) has represented a corruption act, as a payment of the services

performed by the two individuals to the legal representatives of Company Y, in their quality as public functionaries.

From the profits made after the transaction, the two individuals invested a part on the capital market, achieving the stock of shares owned before the transaction, constituted banking deposits and investing on the real estate properties.



Case 2: Fraudulent Bankruptcy

Source: NOPCML

The shareholders of the company X were Individual A, Individual B, Individual C and D (front men of Individual B) and Company A1 (owned by the individual A). Company X obtained from a commercial bank a loan for inventories financing of ROL 40 billions. After two days, Company X concluded a mandate contract without representation with Company A2, through which has empowered Company A2 to invest on the capital market. The shareholders of Company A2 were Individual A, Company X, and Company A3 (also owned by Individual A). On the basis of the mandate contract concluded between Company X and Company A2, Company X transferred ROL 30 billions in the banking accounts of Company A2. The money originated in the banking loan for financing the inventories. Also, another ROL 15 billions have been transferred in the banking account of Company A3, representing the value of the shares owned by Company A3 in Company A2.

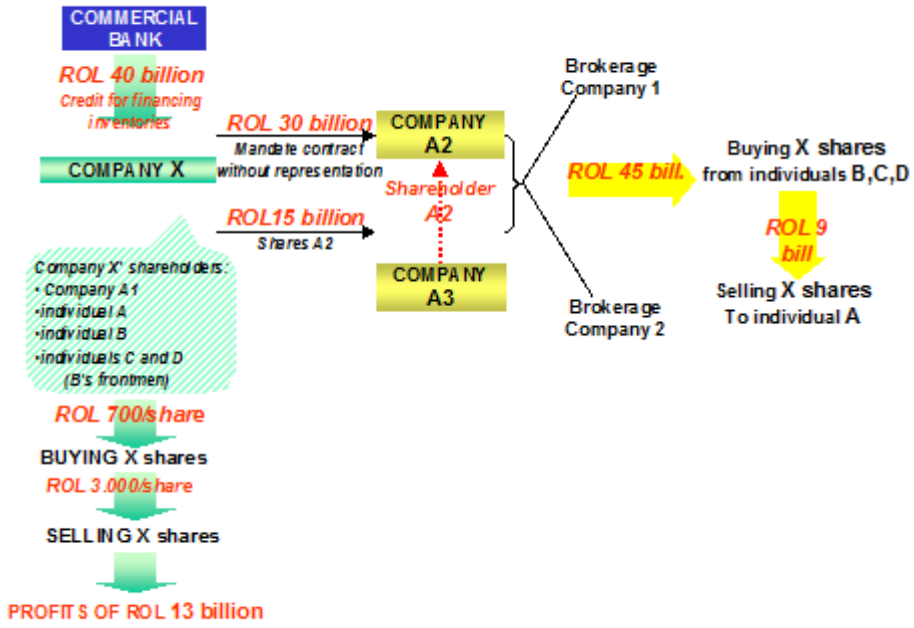
The two companies, A2 and A3, through the means of two brokerage companies have acquired the shares of Individuals B, C and D in Company X. The transaction has been performed through 6 cross transaction, at a price a lot superior than the market price. The entire amount of ROL 45 billions has been used for acquiring the shares owned by Individuals B, C and D in Company X.

Furthermore, two days before concluded the 6 cross transactions, Individuals C and D, enjoying some privileged information, acquired shares of Company X at the market price, and

sold them in the six suspicious transactions at a price approximately 4 times superior, achieving a profit of almost ROL 13 billions.

A day after acquiring shares of Company X, Companies A2 and A3 have sold, at the market price, to the Individual A, a part of the shares owned in Company X.

Using the money of Company X that he administered, Individual A have managed to buy out the other significant individual shareholders (B, C and D), becoming therefore the major shareholder in Company X.



Case 3: Tax Evasion and Embezzlment

Source: NOPCML

An off-shore has established in Romania Company X and Company W.

Company X, having as shareholders the above-mentioned off-shore company and the company W (of whom the single associate is the off-shore company), using successive transfers through several banking accounts, has fed the accounts of Company Y, a shell company, with the total amount of ROL 6.6 billion, from which ROL 2.3 billion representing "value of goods sold" and the remaining ROL 4.3 billion representing "capital increase".

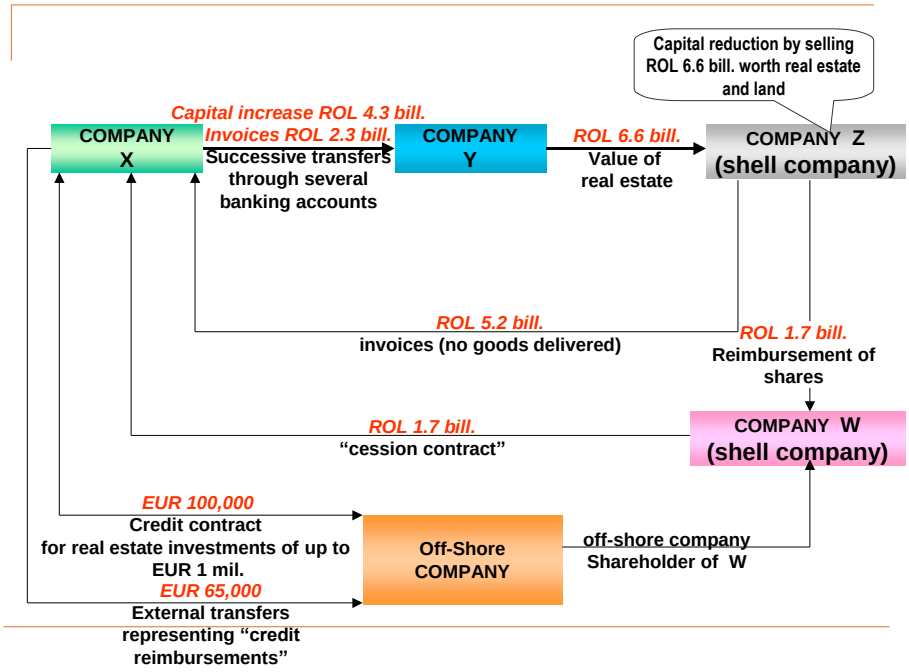
Company Y (listed on the capital market) has bought land and real estate from the Company Z for ROL 6.6 billion. Company Z, a shell company, of whom the shareholders are Company X and Company W, has reduced his social capital by ROL 6.6 billion, through the writing off from the accounting registers of the land and real estate sold to Company Y. From the ROL 6.6 billion transferred by the Company Y for the land and real estate purchased, the Company Z has paid ROL 5.2 billion to Company X, representing "value of goods sold". It was discovered that the merchandise was never delivered, the invoices being false. Another ROL 1.7 billion has been debited from the Company Z' accounts in favor of Company W (shareholder of W Company), representing "reimbursement of shares". The ROL 1.7 billion

have been transferred further from the banking accounts of Company W to the accounts of Company X, with the "cession contract" justification.

Therefore, in the accounts of Company X have entered ROL 6.9 billion.

The initial ROL 6.6 billion that have been debited from Company X' accounts, have been transferred from one of the shareholders of Company X, the off-shore company. The accounts of Company X have been credited with EUR 100,000 as a part of a loan contract for real estate investments of up to EUR 1 million.

After the above mentioned operations, from the company X accounts have been transferred EUR 65,000 in favor of the off-shore company, as "credit reimbursements".



Case 4: Smuggling

Source: FATF

This case is based on the data received from a foreign FIU, regarding the involvement of a company established in their country.

A foreign FIU notified NOPCML about some cross-border transfers amounting USD 5 million, ordered by the foreign company and received by two Romanian citizens in their personal accounts. The transfers were justified as "legal and accountancy consultancy". After the money transfer, both Romanian citizens debited their personal accounts for cash withdrawals, amounting a total of USD 1 million.

It was discovered that citizen B also bought Romanian Treasury bonds amounting USD 2 millions. Romanian Company X benefited of a transfer of USD 125,000 from citizen A, and USD 100,000 from citizen B. Both transfers were justified as "personal contribution to the company owned". After the transfers, the accounts of Company X were frequently debited for cash withdrawals, justified as "fake contracts".

All the cash withdrawals were not evidenced in the Company X' accountancy.

On the correspondence with the foreign FIU that first signalled the operations, it was established that the initial USD 5 million amount was of illicit origin and it was used for recycling. The initial USD 5 million originated from smuggling.

Case 5: Terrorist funds collected in Country A transferred to a terrorist organization in Country B

Source: FATF

A terrorist organization would make use of its overseas contacts to "tax" the expatriate community on their earnings and savings. The tax would go to a "calling fund" and would then be wired to the representative office, which was also the political wing of the group based in the neighboring country.

The neighboring country had a significant cross-border ethnic spread in the "target" country, and weapons and material would be purchased and smuggled across the border into the autonomous province where the terrorist organization carried out its attacks.

Case 6: A terrorist organization uses wire transfers to move money to further its activities across borders

Source: FATF

A terrorist organization in country X was observed using wire transfers to move money in Country Y that was eventually used for paying rent for safe houses, buying and selling vehicles, and purchasing electronic components with which to construct explosive devices. The organization used "bridge" or "conduit" accounts in Country X as a means of moving funds between countries. The accounts at both ends were opened in the names of people with no apparent association with the structure of terrorist organization but who were linked to one another by kinship or similar ties. There were thus the apparent family connections that could provide a justification for the transfers between them if necessary.

Funds, mainly in the form of cash deposits by the terrorist organization were deposited into bank accounts from which the transfers are made. Once the money was received at the destination, the holder either left it on deposit or invested it in mutual funds where it remained hidden and available for the organization's future needs. Alternatively, the money was transferred to other bank accounts managed by the organization's correspondent financial manager, from where it was distributed to pay for the purchase of equipment and material or to cover other ad hoc expenses incurred by the organization in its clandestine activities.

Case 7: An Insurance policy used to launder money

Source: FATF

A money launderer purchased marine property and casualty insurance for a phantom ocean-going vessel. He paid large premiums on the policy and suborned the intermediaries so that regular claims were made and paid.

However, he was very careful to ensure that the claims were less than the premium payments, so that the insurer enjoyed a reasonable profit on the policy.

In this way, the money launderer was able to receive claims cheques which could be used to launder funds. The funds appeared to come from a reputable insurance company, and few questioned the source of the funds having seen the name of the company on the cheque or wire transfer.

Case 8: Money laundering following insurance firm pay outs

Source: FATF

Police in Country A uncovered a case of trafficking in stolen cars where the perpetrators provoked accidents in Country B to be able to claim the damages. The proceeds were laundered via public works companies. A network consisting of two teams operated in two different regions of Country A. Luxury vehicles were stolen and given false number plates before being taken to Country B. An insurance contract was taken out in the first country on these vehicles. In Country B, the vehicles were deliberately written off and junk vehicles with false number plates were bought using false identity documents to be able to claim the damages from the insurance firms in Country A.

Around a hundred luxury stolen vehicles were used in this scheme to claim the damages resulting from the simulated or intentional accidents that were then fraudulently declared to the insurance firms. The total loss was over USD 2.5 million. The country in which the accidents occurred was chosen because its national legislation provided for prompt payment of damages.

On receipt of the damages, the false claimants gave 50% of the sum in cash to the leader of the gang who invested these sums in Country B. The investigations uncovered bank transfers amounting to over USD 12,500 per month from the leader's accounts to the country in question. The money was invested in the purchase of numerous public works vehicles and in setting up companies in this sector in Country B. Investigations also revealed that the leader of the gang had a warehouse in which luxury vehicles used for his trafficking operation were stored. It was also established that there was a business relationship between the leader and a local property developer, suggesting that the network sought to place part of its gains into real estate.

Case 9: Money Launderers use the insurance industry to clean their funds

Source: FATF

Clients in several countries used the services of an intermediary to purchase insurance policies. Identification was taken from the client by way of an ID card, but these details were unable to be clarified by the providing institution locally, which relied on the due diligence checks of the intermediary.

The policy was put in place and the relevant payments made by the intermediary to the local institution. Then, after a couple of months had elapsed, the institution would receive notification from the client stating that there was now a change in circumstances, they would have to close the policy incurring the losses, and would thus request a reimbursement (by cheque).

On other occasions the policy would be left to run for a couple of years before being closed with the request that the payment be made to a third party. This reimbursement cheque was then often processed by the local financial institution without further question since the payment came from another reputable local institution.

Case 10: Organized crime launders money through life insurance policies

Source: FATF

Customs officials in Country X initiated an investigation which identified a narcotics trafficking organisation had utilised the insurance sector to launder proceeds. Investigative efforts by law enforcement agencies in several different countries determined that narcotic traffickers were laundering funds through Insurance firm Z located in an off-shore jurisdiction.

Insurance firm Z offers investment products similar to mutual funds. The rate of return was tied to the major world stock market indices so the insurance policies were able to perform as investments. The account holders would over-fund the policy, moving monies into and out of the fund for the cost of the penalty for early withdrawal. The funds would then emerge as a wire transfer or cheque from an insurance company, and the funds were apparently clean.

To date, this investigation identified that over USD 29 million was laundered through this scheme, of which over USD 9 million dollars has been seized. Additionally, based on joint investigative efforts by Country Y (the source country of the narcotics) and Country Z customs officials, several search warrants and arrest warrants were executed relating to money laundering activities involved individuals associated with Insurance firm Z.

Case 11: An associate of a PEP launders money gained from large scale corruption

Source: FATF

A video tape aired in Country A showed presidential adviser Mr. Z purportedly offering a bribe to an opposition politician. This publicity about Mr. Z, widely regarded as the power broker behind then-President in Country A, led the President to appoint a special prosecutor prompting numerous other investigations in Country A into the illicit activities of Mr. Z and his associates. An investigation initiated by authorities in Country B authorities froze approximately USD 48 million connected to Mr. Z 6 . Mr. Z fled the country and was eventually captured and extradited to Country A to face corruption, drug trafficking, illicit enrichment and other charges.

Prior to the capture of Mr. Z, an associate of Mr. Z, Mr. Y was arrested on a provisional arrest warrant and request for extradition from Country A. Mr. Z and his associates, including Mr. Y, generated the criminal proceeds forfeited in this case through the abuse of Mr. Z's official position as advisor to former the President of Country A. Some of the principal fraudulent schemes involved the purchase of military equipment and service contracts as well as the criminal investment of government pension funds. Mr. Y was involved in a huge kickback scheme that removed money from both Country A's treasury and their military and police pension fund. Mr. Y and others used pension fund money and their own money to buy a majority interest in a Country C banking institution, Bank M, which in June 1999 was bought by another bank in Country A. Mr. Y was in charge of seeking investments on behalf of Bank M and identified construction and real estate projects for the bank and pension fund to finance. He also controlled the construction companies which built those projects. Mr. Y established a pattern of inflating the actual cost of the pension fund investment projects by 25 percent and billed Bank M accordingly. Projects recommended by Mr. Y were automatically approved by the board members at the police pension fund, as several of them received kickbacks. A USD 25 million project was fraudulently inflated by USD 8 million. Similarly, Mr. Y covertly

formed and controlled several front companies used to broker loans from Bank M in exchange for kickbacks from borrowers. When some loans defaulted, Mr. Y would purchase the bankrupt projects at extremely low prices for resale at a profit.

In addition, Mr. Y and members of Bank M's board of directors were authorised by Country A's government to arrange the purchase of military aircraft for the nation. In just two aircraft deals the government of Country A paid an extra USD 150 million, because of a fraudulent 30 percent mark-up added on to the sale price. This illicit money allegedly was funnelled through Bank M. From there, it flowed into numerous accounts under a variety of names in banks in foreign jurisdictions to conceal the origin of the funds.

Mr. Y consistently used a group of banks abroad to launder his and others' share of criminal proceeds. Ms. D, a banker who is married to Mr. Y's cousin, formerly was a member of the board of directors of Bank N, helped Mr. Y conceal more than USD 20 million in one jurisdiction.

Mr. Y opened a bank account in Country C, and moved about USD 15 million through it until he was arrested.

Initially, the account opening did not raise any suspicion because Country A nationals often opened bank accounts in the Country C to protect their assets from inflation. However, financial institutions holding bank and brokerage accounts owned or controlled by Mr. Y, Ms. D and others gradually noticed unusual activity in the accounts. According to bank officials, Mr. Y's financial transactions had no apparent business justifications and the origin of the funds was suspicious.

Case 12: Laundering the proceeds of embezzlement

Source: FATF

The bank accounts of a petroleum minister (Mr. Y) of a former dictatorship under which numerous embezzlement offences had been committed were credited with a sum of USD 6 million in the space of a few months. This provided grounds for the case to be referred to the judicial authorities who decided to indict the minister.

On investigation the FIU discovered that Mr. Y was operating under the cover of an alias. The recently opened account controlled by Mr. Y had been credited with a notary's cheque for over USD 575,000 corresponding to the sale of a property. This sum did not correspond in any way to the market value of the property.

Case 13: Wire transfers are used as part of a terrorist fundraising campaign

Source: FATF

An investigation in Country A of Company Z, a company thought to be involved in the smuggling and distribution of pseudoephedrine (a suspected source of revenue for terrorist organisations), revealed that employees of Company Z were sending a large number of negotiable cheques to Country B. Additional evidence revealed that the target business was acting as an unlicensed money remitter. Based on the above information, search warrants were obtained for the Company Z premises and two residences. Analysis of the documents and bank records seized as a result of the search warrants indicated that the suspects had wire transferred money to an individual with suspected ties to a terrorist group.

Later that year the investigators engaged in a series of coordinated searches. Three subjects were arrested and charged for failure to register as a financial business, and approximately USD 60,000 in cash and cheques were seized. Additionally, a bank account was identified containing approximately USD 130,000, which was used to facilitate the illegal wire transfers to destinations outside Country A. The subjects are currently awaiting trial.

Case 14: Payments are structured to avoid detection

Source: FATF

Over a four year period, Mr. A and his uncle operated a money remittance service known as Company S and conducted their business as an agent of a larger money remitting business that was suspected of being used to finance terrorism. Later an investigation was initiated in relation to Company S based on a suspicious transaction report.

The investigation showed that over the four-year period, Mr. A's business had received over USD 4 million in cash from individuals wishing to transmit money to various countries. When Mr. A's business received the cash from customers, it was deposited into multiple accounts at various branches of banks in Country X. In order to avoid reporting requirement in effect in Country X, Mr. A and others always deposited the cash with the banks in sums less than USD 10,000, sometimes making multiple deposits of less than USD 10,000 in a single day.

Mr. A. was charged and pleaded guilty to a conspiracy to "structure" currency transactions in order to evade the financial reporting requirements.

Case 15: Raising of funds through an NPO

Source: FATF

A registered charity, ostensibly involved in child welfare, used video tapes depicting religious "freedom fighters" in action in various countries, together with graphic images of atrocities perpetrated against members of that religion. The tapes contained an appeal to send donations to a post office box number to help in the "struggle".

These tapes were apparently widely distributed around religious establishments throughout the region. The same post office box number was associated with a further appeal in magazines which published articles by well known extremists.

Case 16: An NPO is used to transfer money to suspected terrorists

Source: FATF

An FIU in Country A obtained updated information from the United Nations Security Council consolidated list of designated persons and entities. One of the organisations on the list conducted its operations under different variations of the same name in a number of countries. It was described as a tax-exempt NPO for which the stated purpose was to conduct humanitarian relief projects throughout the world. Among the multiple locations provided UN list for branches of this organisation, several of the addresses were in Country A.

The FIU received a suspicious transaction report on the NPO listed at one of the addresses indicated by the UN list. The report indicated bank accounts and three individuals with controlling interest on the address in Country A. One of the individuals (Mr. A) had an address that matched one of the addresses indicated on the UN list, and the other two individuals had addresses in two different countries. A search by the FIU revealed that the Mr. A was linked to these organisations, as well as to four other international NPOs. Reports received by the FIU detail multiple wire transfers sent from locations of concern to the branches of the above-mentioned charity and to Mr. A.

Case 17: NPO's used to make illegal transfers

Source: FATF

An on-going criminal investigation into a network of foundations (at least 215 NPO's) established by the members of a particular immigrant community revealed that the network was transferring large sums of money regularly to a few accounts in another country. Suspicious transaction reports from the banks were triggered by the unusually high amount of the transactions in comparison with the stated purpose and activities of the foundations. After an initial analysis, it became clear that one of the beneficiaries of the transactions carried out by these organizations was a company contained in the UN Security Council list of designated persons. The FIU forwarded the case for further investigation by law enforcement agencies.

Although the stated purpose of these foundations was charitable, the size and frequency of the transfers (both through regular bank accounts and by using money transfer services) were difficult to explain. Over a 3-year period, the 35 NPO's sent over USD 160 million overseas. The network consisted of a sizable number of foundations spread throughout the country, with a concentration in cities with a large presence of the same immigrant community. The ongoing criminal investigation concluded that the NPO's were most likely a cover for an alternative remittance system. Although it is still too early to draw a clear conclusion about the source and destination of the funds of this network, there is at least the possibility that the funds were raised within this immigrant community with the deliberate intent to support terrorist acts.

Case 18: Senior members of an NPO use the organisation to fund terrorism

Source: FATF

An NPO was registered in Country X as a tax-exempt charity whose stated purpose is to conduct humanitarian relief projects throughout the world. Although the NPO was incorporated in Country X, it operated in various locations using slightly different names.

Financial and business records were seized from the NPO's head office and the homes of the NPO's chief executive officer and a member of its board of directors. On the same date, Country X issued an order blocking the NPO's assets and records pending further investigation. Eleven months later, Country X submitted the NPO to the UN for designation under relevant UN Security Council resolutions for its support of a terrorist organisation. Country X convicted the chief executive officer of the NPO for fraud and organized crime related offences for diverting more than USD 315,000 of charitable donations to terrorist organisations. Prior to these actions, there is evidence that the NPO had provided both direct and indirect financial support terrorist organisations.

Case 19: A senior government official launders embezzled public funds via members of his family

Source: FATF

The family of a former Country A senior government official, who had held various political and administrative positions, set up a foundation in Country B, a fiscally attractive financial centre, with his son as the primary beneficiary. This foundation had an account in Country C from which a transfer of approximately USD 1.5 million was made to the spouse's joint account opened two months previously in a banking establishment in neighbouring Country D. This movement formed legitimate grounds for this banking establishment to report a suspicion to the national FIU.

The investigations conducted on the basis of the suspicious transaction report found a mention on this same account of two previous international transfers of substantial sums from the official's wife's bank accounts held in their country of origin (A), and the fact that the wife held accounts in other national banking establishments also provisioned by international transfers followed by withdrawals. The absence of any apparent economic justification for the banking transactions conducted and information obtained on the initiation of legal proceedings against the senior government official in his country for embezzlement of public funds led to the presumption, in this particular case, of a system being set up to launder the proceeds of this crime. The official concerned was subsequently stopped for questioning and placed in police custody just as he was preparing to close his bank account. An investigation has been initiated.

Case 20: A senior employee of a state-owned company involved in high level corruption

Source: FATF

An investigation into a senior government official Mr. A, an employee of state owned Company A, uncovered that he was in receipt of excessive payments into a number of accounts that he owned and operated. Mr. A was the vice president of Company A and had a yearly income of over USD 200,000. The investigation revealed Mr. A had 15 bank accounts in several different countries through which over USD 200 million had been transacted.

Mr. A used the money placed in these accounts to gain political influence and to win large contracts from foreign governments on behalf of Company A.

The investigation discovered that a trust account had been created to act as conduit through which payments from Company A were then transferred to a number of smaller accounts controlled by Mr. A. Mr. A would then transfer money from these accounts or make cash withdrawals. The funds, once withdrawn were used to pay for bribes. The recipients of these payments included: heads of state and government, senior government officials, senior executives of state owned corporations and important political party officials in several countries and family members and close associates of Mr. A.

Further investigation into the financial transactions associated with the accounts held by Mr. A revealed that a shell company was being used to make and receive payments. In addition to this regular account activity, there were irregular cash deposits (often more than one a day) and unusually large of cash withdrawals; one account revealed that in one six week period over USD 35 million had been withdrawn in cash. This was inconsistent with all the previous activity on the account. The investigators noticed that there was also a deliberate smurfing of the cash deposits into smaller amounts indicating Mr. A had an awareness of reporting requirements and was

attempting to avoid them. The beneficial owners of payments from Mr. A made both in cash and by wire transfer implicated several PEP's and associates of PEP's:

- The senior politician, senior official. An intermediary received a payment of USD 50 million from Company A. The intermediary then transferred the money into two accounts held offshore; the funds were then moved to company accounts that were also held offshore. The beneficial owners of these company accounts were discovered to be a former head of the secret service in Country B and a state secretary for the Ministry of Defence in Country C.

- Wife of a PEP. Money was transferred from Company A to one of the bank accounts owned by Mr. A; Mr. A then placed funds into a solicitor's client account and an offshore bank account. The beneficial owner of the offshore account was the recently divorced wife of a PEP – Ms. C. The account was provided with funds for the purchase a property valued at over USD 500,000, a car, the redecoration of Ms. C's flat and a monthly allowance of USD 20,000.

- Friend and associate of the PEP. Company A made a payment to a bank account in Country D. The bank in Country D was then instructed to make transfer the money to an associate of Mr. A, who held an account in the same bank in Country D. The associate then 'loaned' the same amount of money to a PEP.

Case 21: Accountant and lawyers assist in a money laundering scheme

Source: FATF

Suspicious flows of more than USD 2 million were identified being sent in small amounts by different individuals who ordered wire transfers and bank drafts on behalf of a drug trafficking syndicate who were importing of 24 kg of heroin concealed in cargo into Country Z. Bank drafts purchased from different financial institutions in Country Y (the drug source country) were then used to purchase real estate in Country Z.

An accountant was used by the syndicate to open bank accounts and register companies. The accountant also offered investment advice to the principals.

A firm of solicitors was also used by the syndicate to purchase the property using the bank drafts that had been purchased overseas after they had first been processed through the solicitor's trust account. Family trusts and companies were also set up by the solicitors

Case 22: Legal professionals facilitate in money laundering

Source: FATF

A director of several industrial companies embezzled several million dollars using the bank accounts of offshore companies. Part of the embezzled funds were then invested in real estate in Country Y by means of non-trading real estate investment companies managed by associates of the person who committed the principal offence.

The investigations conducted in Country Y, following a report from the FIU established that the creation and implementation of this money laundering channel had been facilitated by accounting and legal professionals - gatekeepers. The gatekeepers had helped organize a number of loans and helped set up the different legal arrangements made, in

particular by creating the non-trading real estate investment companies used to purchase the real estate. These professionals also took part in managing the structures set up in Country Y.

Case 23: An accountant provides specialist financial advice to organized crime.

Source: FATF

A law enforcement operation identified an accountant, Mr. J, who was believed to be part of the criminal organisation involved in money laundering and re-investment of illicit proceeds derived from drugs trafficking led by Mr. X. Mr. J's role was mainly that of a "legal and financial consultant". His task was to analyse the technical and legal aspects of the investments planned by the organisation and identify the most appropriate financial techniques to make these investments appear licit from a fiscal stance. He was also to try as much as possible to make these investments profitable. Mr. J was an expert in banking procedures and most sophisticated international financial instruments. He was the actual financial "mind" of the network involved in the re-investment of proceeds available to Mr. X. Mr. J operated by sub-dividing the financial transactions among different geographical areas through triangle transactions among companies and foreign credit institutions, by electronic transfers and stand-by credit letters as a warrant for commercial contracts which were later invested in other commercial activities.

Case 24: A lawyer uses offshore companies and trust accounts to launder money

Source: FATF

Mr. S headed an organisation importing narcotics into country A, from country B. A lawyer was employed by Mr. S to launder the proceeds of this operation. To launder the proceeds of the narcotics importing operation, the lawyer established a web of offshore corporate entities. These entities were incorporated in a Country C, where scrutiny of ownership, records, and finances was not strong. A local management company in Country D administered these companies. These entities were used to camouflage movement of illicit funds, acquisition of assets, and financing criminal activities. Mr. S was the holder of 100% of the bearer share capital of these offshore entities.

In Country A, a distinct group of persons and companies without any apparent association to Mr. S transferred large amounts of money to Country D where it was deposited in, or transited through Mr. S's offshore companies.

This same web network was found to have been used to transfer large amounts of money to a person in Country E who was later found to be responsible for drug shipments destined for Country A; Several other lawyers and their trust accounts were used to receive cash and transfer funds, ostensibly for the benefit of commercial clients in Country A. When they were approached by law enforcement during the investigation, many of these lawyers cited "privilege" in their refusal to cooperate. Concurrently, the lawyer established a separate similar network (which included other lawyers' trust accounts) to purchase assets and place funds in vehicles and instruments designed to mask the beneficial owner's identity. The lawyer has not been convicted of any crime in Country A. Investigators allege however that his connection to and actions on behalf of Mr. S are irrefutable.

Case 25: A solicitor uses his client account to assist money laundering

Source: FATF

Over a period of three years Mr. X repatriated the funds to Country Y for his use and benefit. He was assisted by lawyers and accountants using false transactions and offshore corporations. Mr. Y, formerly a lawyer, facilitated Mr. X's repatriation scheme by managing Mr. X's offshore corporation and bank accounts in several important financial centres. Mr. Y drafted documents that purported to be "loan" agreements between the offshore shell corporation and a Mr. X nominee in Country Y. These loan agreements served as the basis for the transfer of millions from bank accounts in several different countries to the Mr. X's home country. Upon arrival in the bank accounts opened by Mr. X's nominee, the funds were transferred to Mr. X. Mr. Y's lawyer used the law firm's bank accounts to facilitate the transfers

Case 26: A trust fund is used to receive dirty money and purchase real estate

Source: FATF

A lawyer was instructed by his client, a drug trafficker, to deposit cash into the lawyer's trust account and then make routine payments for mortgages on properties beneficially owned by the drug trafficker. The lawyer received commissions from the sale of these properties and brokering the mortgages. While he later admitted to receiving the cash from the trafficker, depositing same into his trust account, and administering payments to the trafficker's mortgages, he denied knowledge of the source of the funds

9. CHALLENGING ISSUES

9.1."Politically Exposed Persons"

Sources:

Phare Project RO99-IB/JH-02 – Training Manual on Anti Money Laundering – 2002

The Wolfsberg Group: Wolfsberg FAQ's on Politically Exposed Persons

The Malaysian Institute of Chartered Secretaries And Administrators - Anti-Money Laundering & Anti-Terrorism Financing - Internal Policy and Procedures Sample

Individuals who have or have had positions of public trust such as government officials, senior executives of government corporations, politicians, important political party officials etc. and their families and close associates require heightened scrutiny.

The term "politically exposed persons" ("PEP") applies to persons who perform important public functions for a state. The definition used by regulators or in guidance is usually very general and leaves room for interpretation. For example the Swiss Federal Banking Commission in its guidelines on money laundering uses the term "person occupying an important public function", the US interagency guidance uses "senior foreign political figure" and the BIS paper Customer due diligence for banks says "potentates".

The term should be understood to include persons whose current or former („Rule of thumb": 1 year after giving up any political function) position can attract publicity beyond the borders of the country concerned and whose financial circumstances may be the subject of additional public interest. In specific cases, local factors in the country concerned, such as the political and social environment, should be considered when deciding whether a person falls within the definition.

The following examples are intended to serve as aids to interpretation:

- Heads of state, government and cabinet ministers;
- Influential functionaries in nationalized industries and government administration;
- Senior judges;
- Senior party functionaries;
- Senior and/or influential officials, functionaries and military leaders and people with similar functions in international or supranational organizations;
- Members of ruling royal families;
- Senior and/or influential representatives of religious organizations (if these functions are connected with political, judicial, military or administrative responsibilities)

The term "families" should include close family members such as spouses, children, parents and siblings and may also include other blood relatives and relatives by marriage.

The category of "closely associated persons" should include close business colleagues and personal advisors/consultants to the politically exposed person as well as persons who obviously benefit significantly from being close to such a person.

Political parties are not covered by the definition "Politically Exposed Person". However, Banks should consider to apply heightened scrutiny to business relationships holding assets of foreign political parties.

Identifying Politically Exposed Persons can be a difficult undertaking, particularly, if the customer fails to provide important information or even gives false information. Despite all the banks' efforts at recognizing Politically Exposed Persons, it is a fact that they do not have the necessary powers, means nor information at their disposal to detect such persons. Banks are restricted in what information they can obtain. They must rely on the information they are given by clients and that can be gleaned from business documents or from the media. In particular, when close associates or families of a Politically Exposed Person open a business relationship with a bank it is often impossible to establish that relationship a "PEP relationship" on the basis of the limited information available to the banks.

The following prompts might - in addition to the standardized KyC procedures - be appropriate to recognize a Politically Exposed Person:

- The question of whether clients or other persons involved in the business relationship (see below) perform a political function should form part of the standardized account opening process, especially in cases of clients from corruption-prone countries.
- To let client advisor deal exclusively with clients from a specific country/region might improve their knowledge and understanding of the political situation in that country/region.

- The issue of Politically Exposed Persons should form part of the regular KyC training programs

- Banks may use databases listing names of Politically Exposed Persons (and their entourage). In this regard it would be helpful if authorities issuing directives on how to deal with Politically Exposed Person would support the banks.

In addition to the generally applicable "Know your customer" rules a detailed approval process ("heightened scrutiny"), including a function independent from the business line (e.g. Compliance) and senior management approval should apply. In addition, such business relationships should be subjected to additional controls and a more detailed examination at least once a year.

Heightened scrutiny has to be applied whenever the Politically Exposed Persons/families/ associates is the contracting party of the Bank or the beneficial owner of the assets concerned, or has power of disposal over said assets by virtue of a power of attorney or signature authorization.

9.2 Non face-to-face business relationships and transactions

Sources:

Basel Committee on Banking Supervision - Customer Due Diligence for banks

Basel Committee on Banking Supervision - Risk Management Principles for Electronic Banking

Wolfsberg AML Principles (Global Anti-Money Laundering Guidelines for Private Banking)

Documentation by the Working Group on the review of the 40 Recommendation

FATF - 40 Recommendations - 2003

EU Commission - Draft for a new Directive on Money Laundering

Financial intermediaries -in particular banks- are increasingly asked to open business relationship -in particular accounts- on behalf of customers who do not present themselves for personal interview. This has always been a frequent event in the case of non-resident customers, but it has increased significantly with the expansion electronic money and of telephone or electronic banking.

Electronic money is a substitute for cash that operators, possibly protected by guarantees of anonymity, can exchange even at a considerable distance, establishing themselves in countries lacking adequate controls. Financial institutions issuing such instruments should work out and apply specific precautions with particular reference to:

- controls on the distribution systems of payment cards and on business companies that accept them as a mean of payment;

- record keeping of requests for refunds of e-money balances that are anomalous by frequency or amount.

Threshold on individual cards and on single transactions, and the impossibility (or at least the traceability) of sums transfers from one electronic cards should be considered by issuing institutions as means to avoid the illicit use of such instruments.

Notably electronic banking incorporates today a wide array of products and services delivered over telecommunications networks. The impersonal and borderless nature of electronic banking combined with the speed of transaction inevitably creates difficulties in customer identification and verification. As consequence, it is necessary for intermediaries to assess various risks posed by emerging technologies and to design customer identification procedures with due regard to such risks. In accepting business from non face-to-face customers banks should apply equally effective identification procedures for non face-to-face customers as for those available for interview and adopt measures to mitigate the risks as:

- certification of presented documents;
- requisition of additional documents to complement those which are required for face-to-face customers;
- independent contact with the customer by the intermediary;
- third party introduction by an introducer subject to analogous customer due diligence standard and ready to supply immediately all relevant identification data and other documentation pertaining the identity and the activity of the introduced party;
- requiring the first payment to be carried out through an account in the customer's name with another intermediary (bank) subject to similar customer due diligence standards.

Transactions performed by such customers (non face-to-face transactions) should be adequately monitored, specially the ones that appear unusual or involve significant transfers; moreover, computer programs can be used to identify anomaly indicators for transactions transmitted by phone or over electronic networks. Statistical observation mechanisms are in fact able to monitor transactions from the point of view of their repetitiveness and of the relevance of the amounts involved.

The 2003 FATF 40 Recommendations consider the problem of non face-to-face business relationships and transactions in the Recommendations 8, where financial institutions are invited to "pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. In particular, financial institutions should have policies and procedures in place to address any specific risks associated with non face-to-face relationships or transactions". Recommendations 9 considers the problem of business relationships introduced by third parties with regards to the possibility for the financial institutions to obtain immediately by the introducer the necessary information and documentation and with regards to the customer due diligence standards of the same introducer.

Analogous measures are now considered in the draft prepared by EU Commission for the new Directive on money laundering.

Supervisors must adopt measures and give practical advice in order to ensure that financial institutions have minimum standards and internal controls that allow them to face the risks arising from non face-to-face business relationships and transactions.

Non face-to-face client

Where it is a non face-to-face client, e.g. the beneficial owners of the proposed new entity sends an agent in their stead, we will take steps to:

- • Ensure that the agent has proper authority to act on behalf of the beneficial owners, e.g. obtain letter from beneficiary authorising the agent to act on their his behalf;

- • Verify the identity of the beneficial owner to the extent that we are satisfied that we know who the beneficial owner is, e.g. obtain certified copies of their identification documents such as identity cards and incorporation documents.

Non-face-to-face identification

If a customer does not appear in person, he/she must be asked to supply sufficient information to support identification. This requires that information supplied by a customer can be supplemented and confirmed by a separate reliable source. Contractual terms and conditions must include customer's consent to establish the correctness of the information provided.

Moving money through a bank account is not a sufficient basis for identification. A bank account opened in a Finnish Bank, can, however, be used as supporting data for identification and to ensure the completeness of the audit trail.

Electronic banking and other services are increasingly using digital signatures or IDs to establish the identity of a customer. These enable the risks associated with identification and the authenticity and security of the transaction to be reduced. Therefore the FSA recommends that parties subject to the obligation to report consider implementing these identification methods as soon as possible.

9.3. Corporate vehicles - Beneficial Ownership

Sources:

Basel Committee on Banking Supervision - Customer Due Diligence for banks

Wolfsberg AML Principles (Global Anti-Money Laundering Guidelines for Private Banking)

Documentation by the Working Group on the review of the 40 Recommendation

UK Treasury Consultation Document - Regulatory impact assessment on Disclosure of beneficial ownership of unlisted companies

FATF - 40 Recommendations - 2003

EU Commission - Draft for a new Directive on Money Laundering

The financial institutions were already required to make any possible effort to identify the persons on whose behalf an account was opened or a transaction conducted, if there were doubts as to whether the customers were acting on their behalf. (FATF Recommendation 11 in the 1990 First Edition of the 40 Recommendations).

In the last years concern increased about the availability of information on the persons that are the true owners and controllers of assets derived from criminal activity. As a matter of fact, experience showed how criminals have increasingly used various types of legal entities or arrangements, as part of the money laundering process, to conceal the origin of their wealth. The concern regards in particular the lack of transparency in the ownership and

control of "corporate vehicles" [6] and the consequent problems for financial institutions in the KYC proceedings and for law enforcement in money laundering investigations. It must be considered that the a.m. vehicles are frequently interwoven and those engaged in illegal activities try to disguise and obscure their beneficial ownership of assets and make it more difficult by creating complex structures of companies and trusts, established in a number of different legislation. Moreover, there are differences with regard to different types of "corporate vehicles" and the degree of risk in a jurisdiction may be higher or lower depending on the existing laws and the systems. In particular are considered as more "risky" vehicles like trusts and legislation allowing the existence of companies with bearer shares but not the possibility to ascertain the transmission of the shares and the ultimate beneficial owner.

Information on the beneficial ownership of "corporate vehicles" is required for a wide range of purposes. It is needed for:

- the prevention and control of money laundering and in particular the obligation of entities to report suspicious transactions;
- the effective investigation and/or prosecution of criminal and civil cases;
- the effectiveness in the exchange of information between different authorities and bodies involved in the contrast to money laundering;
- the freezing and seizing of funds and other assets;
- financial institutions and non-financial entities to undertake proper customer due diligence to minimise reputation risk and other risks;
- facing the financing of terrorism, terrorist acts and organisations.

Therefore, the main relevant measures considered at international level (and in particular by FATF in the 2003 Edition of the 40 Recommendations) are:

- Financial Institutions and non financial business must be vigilant in preventing the abuse of corporate vehicles by natural persons ad a "de facto" method of operating anonymous accounts;
- There must be proper identification of the natural persons who are the ultimate beneficial owners and financial institution and non-financial entities must have access to this information;
- Particular care should be taken when "corporate vehicles" has overly complex ownership structures that do not serve a legitimate purpose;
- Financial institutions and non-financial business should understand the structure and the purpose of the "corporate vehicle", determine the source of funds and identify the ultimate natural persons who are the ultimate beneficial owners;

[6] The FATF definition of "corporate vehicles" is based on the 2001 OECD Report on the matter and covers:

- Corporations
  - private (or public) limited companies whose shares are not traded on a stock exchange;
  - international business companies/exempt companies.
- Trusts
- Foundations
- Limited partnerships and limited liability partnerships

- Particular care should be taken where the "corporate vehicle" is incorporated or administered in a jurisdiction that does not provide for a system satisfying the AML requirements.

With reference to the last point, it is evident that in the commercial law field should be present provisions in compliance with the requirements internationally considered as prerequisite conditions to face the problem of beneficial ownership for anti-money laundering purposes.

In the draft prepared by the EU Commission for the new Directive on money laundering it is established that the beneficial owner of legal persons should be identified merely on the basis of the controlled percentage of share capital.

Annex 1

Definition of a Financial Intelligence Unit

Sources:

The World Bank – Reference Guide to Anti Money Laundering and Combating the Financing of Terrorism - 2004

FATF - Web Site – Documents

Egmont Group of Financial Intelligence Units (Egmont Group), which is the international standard setter for FIUs, adopted the following definition of an FIU in November 1996:

A central, national agency responsible for receiving (and, as permitted, requesting), analyzing, and disseminating to the competent authorities, disclosures of financial information (i) concerning suspected proceeds of crime, or (ii) required by national legislation or regulation , in order to counter money laundering.

The United Nations Convention against Transnational Organized Crime (2000) (Palermo Convention) adopted this definition, stating, "Each state Party…shall…consider the establishment of a financial intelligence unit to serve as a national center for the collection, analysis and dissemination of information regarding potential money laundering."

Expanding on this definition, FATF requires countries to establish an FIU, which has these three essential functions, i.e., the collector or "repository" of reported information, analysis and financial information sharing for detecting and countering money laundering and terrorist financing. The FATF also has a general requirement that all national authorities exchange information and co-operate with their domestic and international counterparts.

In 2004, the Egmont Group revised its definition of an FIU to include specifically the combating of terrorist financing.10 The current definition of an FIU as follows:

A central, national agency responsible for receiving (and as permitted, requesting), analyzing and disseminating to competent authorities, disclosures of financial information:

- concerning suspected proceeds of crime and potential financing of terrorism, or
- required by national legislation or regulation, in order to combat money laundering and terrorist financing.

As a result, the Egmont Group's definition of an FIU is entirely consistent with *The Forty Recommendations*.

Core Functions

FIUs vary from country to country, but all of them share three core functions; they receive, analyze and disseminate information to combat money laundering and terrorist financing. The dissemination of financial information should be done on both a domestic and international basis.

Because money laundering is often a cross-border activity, it is important for FIUs to join forces with other national intelligence units. Thus, even the best domestic laws and regulations against money laundering, including those for an FIU, need an effective international information sharing mechanism in order to combat effectively money laundering and terrorist financing.

1. Centralized Repository of Reported Information

Financial institutions must report all suspicious activity reports and other required disclosures (such as cash transaction reports) to their country's FIU. The centralization of this "repository function" – designating the FIU as the recipient of financial disclosures – is a prerequisite for an effective preventive national and international framework against money laundering.

The use of a centralized repository for the reporting of information and required disclosures ensures that all of the relevant information is in one place, facilitating the processing of information and analysis on a consistent basis. Centralization also ensures greater efficiency in information gathering.

2. Analytical Function

FIU's are more than mere databases for financial information required to be submitted by legislation or national regulatory authorities. FIU's must analyze the data they receive because so many suspicious transaction reports (STR's) and other financial disclosures often appear to be innocent transactions.

Ordinary deposits, withdrawals, fund transfers, or the purchase of a security or an insurance policy may, however, be important pieces of information in detecting and prosecuting money laundering and terrorist financing.

Only through examination and analysis can FIUs detect criminal financial transactions. Distinguishing truly suspect transactions from those that are only benignly unusual requires informed analysis. Without it, the most sophisticated data gathering in the world will not be productive.

These analytical functions require countries to vest their FIU's with the necessary legal authority, proper human resources, and sufficient technical capacity. In particular, the FIU's analytical functions require extended powers to access information. These powers should include: access to certain commercial or government databases; the authority to request additional information from reporting entities and other sources as necessary; and access to advanced intelligence techniques and apparatus, such as wire tapping and covert operations, subject to domestic legal principles.

Each country must balance very real privacy concerns against the FIU's need for an effective analytical function. While utilizing publicly available commercial databases does not raise privacy concerns, authorizing centralized intelligence units to request additional information does. The same caution applies to FIU surveillance and other intelligence techniques. Financial institution privacy laws should be drafted so as not to interfere with there functions of the FIU, yet protect the privacy of information.

FIU's perform three specialized analytical functions: tactical, operational and strategic.

a. Tactical Analysis

Tactical analysis is the process of collecting the data needed to build a case and to provide the accompanying facts behind the commission of a criminal offense. Although tactical analysis may be performed on all incoming reports, it is likely that STRs will provide the most directly useful information.

Tactical analysis includes the matching of data received from reporting institutions and others with data held by the FIU or accessible to it. Such data includes lists of names, addresses, phone numbers, and data in the other reports forwarded by reporting institutions. While some reporting institutions produce the simplest form of tactical information themselves, FIU's add to these reports related information on the reported client or transaction that they have in their databases.

Upon receipt of an STR, staff of the FIU will look for additional information on the subject, the company, the transactions, or other elements involved in a particular case to provide the basis for further analysis. The main sources of such additional information are:

- The FIU's own data,
- Publicly available sources,
- Government-held databases,
- Additional information from reporting entities and other entities, and
- Other FIU's.

b. Operational Analysis

Operational analysis uses tactical information to formulate different hypotheses on the possible activities of a suspected criminal. Operational analysis supports the investigative process. It uses all sources of information available to the FIU to produce activity patters, new targets, relationships among the subject and his or her accomplices, investigative leads, criminal profiles, and, where possible indications of possible future behaviour.

One technique of operations analysis is financial profiling. This provides the analyst with methods for developing indicators of concealed income of an individual, a group of individuals, or an organization. It is an effective indirect method of gathering, organizing, and presenting evidence related to the financial status of subjects. The relevance of the profile is to show that the target cannot demonstrate a legitimate source for the difference between his or her outflow of cash versus the income. The tracing of a person's assets may also provide leads linking the subject with predicate offenses.

Through operational analysis, the information received by the FIU is developed into operational intelligence, which can be transmitted to law enforcement agencies or prosecutors for further action.

c. Strategic Analysis

Strategic analysis develops knowledge to be used for the future work of the FIU. The main characteristic of strategic intelligence is that it is not related to individual cases, but rather to new issues or trends. The scope of any strategic analysis varies greatly depending upon the FIU's mandate. It may consist of the identification of evolving criminal patterns in a particular group or the provision of broad insights into emerging patterns of criminality at the national level.

Strategic analysis is developed after all available information has been collected and analyzed. It requires a wider range of data than operational analysis, as well as experienced analysts. The data comes from reports provided by the reporting entities, the FIU's own operational intelligence and tactical information, public sources, law enforcement and other governmental agencies. At a broader level, strategic analysis may suggest the need to impose reporting and other AML/CFT obligations on new entities or enhance existing reporting requirements.

3. Domestic Information Sharing

If it suspects money laundering or the financing of terrorism, the FIU should have the authority to share, or route, financial information and intelligence to other domestic authorities for investigation or action. The FIU should also be authorized to cooperate and coordinate its actions with the other domestic authorities devoted to the detection, prevention and prosecution of money laundering and terrorist financing.

The importance of timely information sharing with the proper authorities cannot be overstated. Effective measures against money laundering rely on getting the available information to the appropriate authority. For most FIU's, the sharing of information usually follows some analysis of reported financial disclosures. For other FIU's, especially those that receive an enormous volume of financial disclosures, the financial disclosures are made available to law enforcement authorities immediately; these FIU's conduct analysis on financial disclosures and other financial information upon request of law enforcement as needed at a later time. In either case, the key is for the FIU to provide the competent authority with financial intelligence as quickly as possible so that the competent authority can pursue the leads provided by the FIU.

Domestic coordination is vital. The FIU has to be an essential partner in domestic coordination and could even be empowered to assume the lead role in coordinating the relevant authorities that fight money laundering – which is to say, the FIU, regulators and supervisors of the financial sector, the police, the judicial authorities, and other relevant ministries or administrations.

4. International Information Sharing

Because so much of money laundering and terrorist financing are cross-border activities, FIU's must be able to share financial intelligence with other FIU's worldwide in order to be effective partners in the international fight against these crimes. A core feature of an FIU is its ability to cooperate in an efficient and rapid manner with all of its foreign counterparts. Information sharing at the international level should occur through direct and secure communication with the competent foreign authorities.

5. Information and Feedback

It is important that the FIU work closely with reporting entities and persons, as well as a country's competent authorities, to fight money laundering and terrorist financing. Consistent with its privacy obligations, the FIU should provide feedback about money laundering

and terrorist financing trends and typologies that will assist financial institutions and non-financial businesses and persons to improve their AML/CFT practices and controls and, in particular, their reporting of suspicious transactions. It is a frequent criticism by reporting institutions that they receive little or no feedback from their FIU's about the usefulness of their reports. Thus, reporting entities have no guidance about whether their approach to reporting is helpful in the fight against money laundering and terrorist financing.

While there are obviously constraints on what an FIU can tell a reporting institution about a particular report (especially if that report involves an ongoing enquiry), it should be possible for the FIU to give general feedback to institutions about the quality and usefulness of their reports. FIU's will also have collected data, which once analyzed, should produce useful information about developments and trends in money laundering. This should be shared with reporting entities and persons so that they know what to look out for in designing their AML/CFT systems. Feedback about particular case histories, once any investigation and legal proceedings are over, should also prove useful.

The FATF now provides that all competent authorities, including FIU's, should establish guidance and provide feedback.38 Authorities can expect this issue to feature prominently in AML/CFT assessments. FIU's will also need to maintain comprehensive statistics on STR's received and disseminated.

Annex 2

International Institutional co-operation in AML and CTF

Sources:

Phare Project RO99-IB/JH-02 – Training Manual on Anti Money Laundering – 2002

The World Bank – Reference Guide to Anti Money Laundering and Combating the Financing of Terrorism - 2004

FATF - Web Site – Documents

The Financial Action Task Force

The Financial Action Task Force on Money Laundering

The Financial Action Task Force on Money Laundering (FATF) is an intergovernmental body whose purpose is to develop and promote an international response to combat money laundering. In October of 2001, FATF expanded its mission to include combating the financing of terrorism.

FATF is a policy-making body, which brings together legal, financial and law enforcement experts to achieve national legislation and regulatory AML and CFT reforms. Currently, its membership consists of 29 countries and territories and two regional organizations. In addition, FATF works in collaboration with a number of international bodies and organizations. These entities have observer status with FATF, which does not entitle them to vote, but otherwise permits full participation in plenary sessions and working groups.

In response to mounting concern over money laundering, the Financial Action Task Force on Money Laundering (FATF) was established by the G-7 Summit that was held in Paris in 1989.

The Task Force was given the responsibility of examining money laundering techniques and trends, reviewing the action, which had already been taken at a national or international level, and setting out the measures that still needed to be taken to combat money laundering. In April 1990, less than one year after its creation, the FATF issued a report containing a set of Forty Recommendations, which provide a comprehensive plan of action needed to fight against money laundering.

During 1991 and 1992, the FATF expanded its membership from the original 16 to 28 members. Since then FATF has continued to examine the methods used to launder criminal proceeds and has completed two rounds of mutual evaluations of its member countries and jurisdictions. It has also updated the Forty Recommendations to reflect the changes which have occurred in money laundering and has sought to encourage other countries around the world to adopt anti-money laundering measures. In 2001, the development of standards in the fight against terrorist financing was added to the mission of the FATF.

FATF's three primary functions with regard to money laundering are:

1. monitoring members progress in implementing anti-money laundering measures;
2. reviewing and reporting on laundering trends, techniques and countermeasures; and

3. promoting the adoption and implementation of FATF anti-money laundering standards globally.

The Forty Recommendations on Money Laundering

FATF has adopted a set of 40 recommendations, *The Forty Recommendations*, which constitute a comprehensive framework for AML and are designed for universal application by countries throughout the world. *The Forty Recommendations* set out principles for action; they permit a country flexibility in implementing the principles according to the country's own particular circumstances and constitutional requirements. Although not binding as law upon a country, *The Forty Recommendations* have been widely endorsed by the international community and relevant organizations as the international standard for AML,

The Forty Recommendations are actually mandates for action by a country if that country wants to be viewed by the international community as meeting standards.

The FATF has also elaborated various Interpretative Notes which are designed to clarify the application of specific Recommendations and to provide additional guidance.

The Eight Special Recommendations on Terrorist Financing

After the tragic events that took place in the United States on 11 September 2001, governments world-wide called for an immediate and co-ordinated effort to detect and prevent the misuse of the international financial system by terrorists. At an extraordinary plenary meeting on the financing of terrorism held in Washington, DC, in October 2001, the FATF thus expanded its mission beyond money laundering to focus its energy and expertise on a world-wide effort to combat terrorist financing. The FATF issued new international standards for combating terrorist financing – the Eight Special Recommendations – and called on all countries to adopt and implement them. Implementing these Special Recommendations will deny access for terrorists and their supporters to the international financial system.

Monitoring Members Progress

In the self-assessment exercise, every member country provides information on the status of its implementation of the Forty Recommendations and Eight Special Recommendations by responding each year to a standard questionnaire. This information is then compiled and analysed, and provides the basis for assessing the extent to which the Recommendations have been implemented by both individual countries and the group as a whole.

The second element for monitoring the implementation of the Forty Recommendations is the mutual evaluation process. Each member country is examined in turn by the FATF on the basis of an on-site visit conducted by a team of three or four selected experts in the legal, financial and law enforcement fields from other member governments. The purpose of the visit is to draw up a report assessing the extent to which the evaluated country has moved forward in implementing an effective system to counter money laundering and to highlight areas in which further progress may still be required.

Monitoring the progress of members to comply with the requirements of *The Forty Recommendations* is facilitated by a two-stage process: self assessments and mutual evaluations. In the self-assessment stage, each member responds to a standard questionnaire, on an annual basis, regarding its implementation of *The Forty Recommendations*. In the

mutual evaluation stage, each member is examined and assessed by experts from other member countries.

In the event that a country is unwilling to take appropriate steps to achieve compliance with The Forty Recommendations, FATF recommends that all financial institutions give special attention to business relations and transactions with persons, including companies and financial institutions, from such non-compliant countries and, where appropriate, report questionable transactions, i.e., those that have no apparent economic or visible lawful purpose, to competent authorities. Ultimately, if a member country does not take steps to achieve compliance, membership in the organization can be suspended. There is, however, the process of peer pressure before these sanctions are enforced.

Reporting on Money Laundering Trends and Techniques

One of the FATF's functions is to review and report on money laundering trends, techniques and methods (also referred to as typologies).

Money laundering and terrorist financing techniques are examined each year at a "typologies" meeting. This provides a forum for law enforcement and regulatory experts from FATF member countries, together with certain international organisations and bodies, as well as representatives from other countries, to discuss the prevailing methods, the emerging threats, and any effective countermeasures that have been developed.

FATF issues annual reports on developments in money laundering through its Typologies Report. These reports are very useful for countries to keep current with new techniques or trends to launder money and for other developments in this area.

The NCCT List

One of FATF's objectives is to promote the adoption of international AML/CFT standards for all countries. Thus, its mission extends beyond its own membership, although FATF can only sanction its member countries and territories. Thus, in order to encourage all countries to adopt measures to prevent, detect and prosecute money launderers, i.e., to implement The Forty Recommendations, FATF has adopted a process of identifying those jurisdictions that serve as obstacles to international co-operation in this area. The process uses 25 criteria, which are consistent with The Forty Recommendations, to identify such non-cooperative countries and territories (NCCT's) and place them on a publicly available list.

An NCCT country is encouraged to make rapid progress in remedying its deficiencies. In the event an NCCT country does not make sufficient progress, counter-measures may be imposed. Counter measures consist of specific actions by FATF member countries taken against an NCCT-listed country. In addition to the application of applying special attention to business relationships and transactions from such countries, the FATF can also impose further counter-measures, which are to be applied in a gradual, proportionate and flexible manner; these include:

- stringent requirements for identifying clients and enhancement of advisories, including jurisdiction-specific financial advisories, to financial institutions for identification of the beneficial owners before business relationships are established with individuals or companies from these countries;

- enhanced relevant reporting mechanisms or systematic reporting of financial transactions on the basis that financial transactions with such countries are more likely to be suspicious;
- in considering requests for approving the establishment in FATF member countries of subsidiaries or branches or representative offices of banks, taking into account the fact the relevant bank is from an NCCT;
- warning non-financial sector business that transactions with entities within the NCCTs might run the risk of money laundering.

Finally, these counter measures may include FATF-member countries terminating transactions with financial institutions from such a country. Most countries make a concerted effort to be taken off the NCCT list because it causes significant problems to their financial institutions and businesses with respect to international transactions, as well as their reputation internationally.

Methodology for AML/CFT Assessments

Throughout 2002, FATF, The international Monetary Fund (IMF), the World Bank, and the other standard setters, in consultation with the FSRB's, worked on a methodology to assess The Forty Recommendations and Special Recommendations, and completed a comprehensive assessment methodology. At its plenary session in October of 2002, FATF adopted this single, comprehensive methodology to be used in making its mutual assessments.

The development of the comprehensive methodology is intended to fill a gap in assessment procedures. First, it is intended to facilitate a more uniform approach world-wide in conducting assessments based on The Forty Recommendations and Special Recommendations. Second, it provides a framework to integrate the work of the different standard setters, as it pertains to AML/CFT, and there has been extraordinary international cooperation and agreement in this regard among the standard setters. Third, the development of the methodology provides a framework for acceptance of The Forty Recommendations and Special Recommendations as the twelfth standard recognized by the IMF and Bank as useful to their operational work, and where Reports on standard and Codes (ROSC's) would be prepared.

The methodology has now been approved by all of the relevant parties that will be making assessments. The methodology consists of 120 criteria covering each of The Forty Recommendations and Special Recommendations. It covers the legal and institutional AML/CFT framework for a country, including financial intelligence units. The methodology also includes relevant elements from United Nations Security Council Resolutions and international conventions, as well as supervisory and regulatory standards for the banking, insurance and securities sectors. It also addresses implementation of the AML/CFT regime in the non-prudentially regulated sector.

The Egmont Group

The fight against money laundering has been an essential part of the overall struggle to combat illegal narcotics trafficking, the activities of organized crime, and more recently the financing of terrorist activity. It became apparent over the years that banks and other financial institutions were an important source for information about money laundering and other financial crimes being investigated by law enforcement. Concurrently, governments around the world began to recognise the corrosive dangers that unchecked financial crimes posed to their economic and political systems.

To address that threat, a number of specialised governmental agencies were created as countries around the world developed systems to deal with the problem of money laundering. These entities are now commonly referred to as "financial intelligence units" or "FIUs". They offer law enforcement agencies around the world an important avenue for information exchange.

Despite the fact that FIUs were created in several jurisdictions throughout the world during the first years of the 1990s, their creation was still seen as isolated phenomena related to the specific needs of those jurisdictions establishing them. Since 1995, a number of FIUs began working together in an informal organization known as the Egmont Group (named for the location of the first meeting at the Egmont-Arenberg Palace in Brussels on 9 June 1995).

The goal of the Egmont Group is to provide a forum for FIUs to improve support to their respective national anti-money laundering programs.

The Egmont Group has approved the following definition of a FIU as of June 2004: Recognising the benefits inherent in the development of a FIU network, in 1995, a group of FIUs at the Egmont Arenberg Palace in Brussels decided to establish an informal group for the stimulation of international co-operation. Now known as the Egmont Group, these FIUs meet regularly to find ways to cooperate, especially in the areas of information exchange, training and the sharing of expertise.

There are currently 94 countries with recognised operational FIU units, with others in various stages of development. Countries must go through a formal procedure established by the Egmont Group in order to be recognised as meeting the Egmont Definition of an FIU. The Egmont Group as a whole meets once a year. Since the Egmont Group is not a formal organiation, there is no permanent secretariat. Administrative functions are shared on a rotating basis. Aside from the Egmont Support position, Working Groups and the Egmont Comittee are used to conduct common business. FIUs, at a minimum, receive, analyse, and disclose information by financial institutions to competent authorities of suspicious or unusual financial transactions.

Although every FIU operates under different guidelines, most FIUs, under certain provisions, can exchange information with foreign counterpart FIUs. In addition, many FIUs can also be of assistance in providing other government administrative data and public record information to their counterparts, which can also be very helpful to investigators. One of the main goals of the Egmont Group is to create a global network by promoting international co-operation between FIUs.

The ongoing development and establishment of FIUs exemplify how countries around the world continue to intensify their efforts to focus on research, analysis and information exchange in order to combat money laundering, terrorist financing and other financial crimes.

Annex 3

The cooperation of the NOPCML with the institutions involved in this area at national level

The need for inter-institutional co-operation, legal framework and the entities involved.

The financial control and penal investigation emphasized the fact that on the Romanian territory exists criminal groups which, using phantom companies or companies with apparent legal activity, commit illegal funds generating offences, funds which are ultimately going through the "laundering" process. Taking into account the financial crime trends, namely to take over more and more the economic sector, badly disturbing the business area, there is a need for a closer cooperation between the institutions involved, in accordance with their competence, in order to combat this flagellum.

For this reason, the provisions of the Law no. 656/2002 on the prevention and sanctioning the money laundering creates the adequate legal framework of a fruitful cooperation of the Office with the entire system of institutions and entities involved in preventing and combating money laundering:

- Institutions having tasks of drawing up/or and enforcing the legislation in the AML field: Ministry of Justice, Ministry of Public Finances, Ministry of European Integration, Ministry of Administration and Interior, the General Prosecutor Office by the High Court of Cassation and Justice, National Bank of Romania, Romanian Intelligence Services, Foreign Intelligence Services;

- Authorities with financial control and prudential supervision attributions: Financial Guard, National Authority for Customs, Public Finance Administration, Court of Account, Supervision Directorate within the NBR, the Licensing and Authorizing Committee for Gambling within the Ministry of Public Finances, National Securities Commission, Insurance Supervisory Commission;

- Entities with reporting obligations: banks and foreign banks branches, financial and credit institutions, insurance and reinsurance companies, economic agents performing gambling or pawning activities, natural and legal persons providing legal, notaries, accounting, financial and banking advice, post offices, foreign exchange offices ("bureaux de change");

- Professional Associations: Romanian Banks Associations, National Associations of Securities Companies, Romanian Bar Association, Romanian Notaries Association and Romanian Accounting and Licensed Experts Body.

The need for inter-institutional cooperation was highlighted through the organization way of the NOPCML itself.

As a result, the debating and decisional structure, the Board, consist in one representative of each of the following institutions: Ministry of Public Finances, Ministry of Justice, Ministry of Administration and Interior, the General Prosecutor Office by the High Court of Cassation and Justice, National Bank of Romania, Court of Accounts and Romanian Banks Association, all appointed by Governmental Decision for a period of 5 years.

Beside the specific activities within the Office, the Board members have also the role to ensure the most efficient way of cooperation with the institutions they are coming from.

Having regard the relevant legal provisions, the Office has taken the lead in coordination of national AML efforts. This fact has been also highlighted in the Evaluation Report on AML/ CTF measures prepared by the experts team of the International Monetary Fund/World Bank in July 2003, mentioning "the FIU has taken the lead in coordination of national AML efforts, became operationally quickly after its creation, and was organized in a manner to maximize inter-agency coordination among supervisory and law enforcement authorities." Also, the Office acts as a buffer to protect confidential financial information, taking into account the way the notifications are submitted to the Prosecutor's Office by the High Court of Cessation and Justice, when suspicious grounds exists regarding the performance of the money laundering offence.

The concrete ways of inter-institutional cooperation promoted by the Office

In order to establish the most adequate ways of cooperation within the specific legal framework applicable to each institution, there have been signed inter-institutional coopeation agreements with the following institutions: Ministry of Public Finances, General Police Inspectorate, Romanian Court of Accounts, National Office for Commerce Register, Insurance Supervisory Commission, Romanian Intelligence Service, Foreign Intelligence Service

The results of development of the Office's cooperation with public institutions and other domestic entities

The activity of the Office cannot be conceived without the cooperation with other domestic authorities and institutions as the Office main tasks are: (i) receiving information through CTR/STR or cross-border reports, (ii) enriching them with information from other institutions or from its own database, (iii) analysing and processing them in order to inform the Prosecutor's Office by the High Court of Cessation and Justice, when suspicious grounds of money laundering arises.

As we already pointed out, in order to minimize the period of and assuring the access to a complete range of information, the Office succeeded to establish on-line access to other public institutions databases, out of which we are mentioning:

- The National Office for Commerce Register, for the entire database of the recorded legal persons;
- Ministry of Public Finances, for the databases regarding the balance sheets, VAT Reimbursement database and the database concerning payment obligations to the State Budget;
- National Customs Authority, for databases regarding custom operations (imports and exports).

Also, there is under implementation on-line access with the General Police Inspectorate for data and computerized evidences of the natural persons and with the National Printing House for information on juridical persons that purchases special regime documents.

These measures leads to an increasing of the quality of the analysis performed within the Office and a minimization of the period needed for analysis, meaning that the Prosecutor's Office could be informed in a very short time on the activities for which there are serious grounds of money laundering.

ANNEX 4

OTHER ROMANIAN SUPERVISING INSTITUTIONS AND PUBLIC BODIES INVOLVED IN AML/CFT ACTION

I. The *National Bank Of Romania (NBR)*

The ***National Bank of Romania (NBR)*** , established in 1880, is the country's central bank.

The National Bank of Romania is an independent public institution with its headquarters in Bucharest. It is the sole institution vested with the power to issue notes and coins to be used as legal tender on the territory of Romania.

The domestic currency is the leu, with its fractional coin, the ban.

Pursuant to Law No. 312/2004 on the Statute of the National Bank of Romania, the NBR's primary objective is to ensure and maintain price stability.

The main tasks of the National Bank of Romania are the following:

- to define and implement the monetary policy and the exchange rate policy;
- to conduct the authorization, regulation and prudential supervision of credit institutions and to promote and oversee the smooth operation of the payment systems with a view to ensuring financial stability;
- to issue banknotes and coins as legal tender on the territory of Romania;
- to set the exchange rate regime and to supervise its observance;
- to manage the official reserves of Romania.

Without prejudice to its primary objective of ensuring and maintaining price stability, the National Bank of Romania supports the general economic policy of the Government.

By law, the National Bank of Romania is solely accountable to Parliament and is on no account subordinated to Government; its relationship with the latter is co-operation on a regular basis.

The National Bank of Romania is managed by a Board of Directors appointed by the Parliament of Romania on the recommendation of the standing committees of the two Chambers of the Parliament. Board members are appointed for a five-year tenure that can be subject to renewal.

The main tasks of the Board of Directors are to decide on the monetary and exchange rate policies, as well as on the measures for authorization, regulation and prudential supervision of the credit institutions and oversight of the authorized payment systems.

II. The Insurance Supervisory Commission

The ***Insurance Supervisory Commission*** is an independent authority, which actively seeks to protect the insured's rights and to promote a stable environment for the Romanian

insurance market. Its mission is to impartially enforce the insurance legislation, with readiness and honesty; to protect, in accordance with the law, the insured from insurance products; to encourage the creation of a healthy insurance market; to promote the necessity to serve public interest.

To this end, the highest standards of ethics and workmanship will be imposed in all formal and informal relationships with individuals, agencies and companies on whom the Commission's policies and actions have an effect upon. The Insurance Supervisory Commission has its foundations in the Law no. 32/2000 regarding the insurance companies and insurance supervision, published in the first part of the Romanian Official Journal on the 10'th of April 2000 and all the subsequent norms and decisions.

In accordance with the commitments assumed by the Insurance Supervisory Commission in Romanian Position Paper presented in Brussels on 2001 year, for chapter 3 – „Freedom to provide services", the Law no. 32/2000 regarding the insurance companies and insurance supervision was amended and completed according to the European Union directives for insurance field.

In accordance with articles 5 and 8 from Law no. 32/2000 regarding the insurance companies and insurance supervision, The Insurance Supervisory Commission has the following functions:

- elaborates or decides upon draft legislation concerning the insurance field and suggests individual administrative acts if related to the insurance business;
- ensures consumer's protection by supervising the insurers' financial situation, and if required carries out inspection on insurers or insurance brokers;
- supervises accounting systems and accounting norm and regulations, after consultation with the professional bodies of insurance companies;
- takes all necessary steps to ensure that the insurance activity is conducted in accordance with specific prudential regulations;
- participates in international associations of insurance supervision authorities;
- elaborates norms in enforcing of Law no. 32/2000 concerning insurance companies and insurance supervision, regarding classes of insurance, insurers and insurance broker authorization procedure, solvency margins, insurers' insolvency, regulations for life insurance funds administration, regulations for investments and asset valuation;
- gives, suspends or cancels official authorizations, approves division or merger of an insurer registered in Romania, approves the transfer of portfolios and gives penalties to insurance companies and brokers which are breaking the legislation in insurance field.

III. The National Securities Commission

The ***National Securities Commission***, hereinafter called the "NSC" or the Commission, is an autonomous administrative authority, enjoying legal personality.

The National Securities Commission regulate and supervise the capital market, the regulated commodity and financial derivative instruments markets, as well as their specific institutions and operations.

The National Securities Commission is subordinated to Parliament and submits reports through the Budget, Finance and Banks Commissions of the Senate and of the Chamber of Deputies.

The National Securities Commission exercises its authority throughout the territory of Romania.

The National Securities Commission have its main registered office located in Bucharest and may open representative offices depending on its necessities.

The basic objectives of the National Securities Commission shall be to:

a. draw up and maintain the necessary framework for the development of regulated markets;

b. promote trust in regulated markets and in financial instruments investments;

c. ensure the protection of operators and of investors against unfair, abusive and fraudulent practices;

d. promote a fair and transparent operation of the regulated markets;

e. prevent market manipulation and fraud and to ensure the integrity of regulated markets.

f. establish standards of financial soundness and honest practice in the regulated markets.

g. take all the necessary actions in order to avoid the generation of a systemic risk on the regulated markets.

h. prevent damaging the equality of notification and treatment of investors or the interests thereof.

IV. The Body of Expert Accountants and Licensed Accountants in Romania

The ***Body of Expert Accountants and Licensed Accountants in Romania***, is an autonomous legal entity of public utility, consisting of expert accountants and licensed accountants, under the conditions provided for by the law.

The Body, by means of the delegation received on behalf of the public authorities, grants and withdraws the right to practice the profession of expert accountant and licensed accountant and has the right to control the competence and the morality of its members.

According to the norm act of establishment, the members of the Body elect the managing bodies to represent them in front of the public authorities, as well as in their relationships with domestic and foreign physical and legal entities.

The managing boards of the Body are the National Conference, hereinafter called the National Conference, the Superior Council of the Body, hereinafter called the Superior Council, and the Standing Board of the Superior Council, hereinafter called the Standing Board.

The National Conference is the superior running and control board of the Body. It includes the members of the Superior Council, the members of the branch councils, members of the discipline commissions, representatives of the Ministry of Finance by the Superior Council and of the branch boards, as well as 1 representative at every 100 members of each branch. The latter shall be designated by the general assemblies.

The National Conference has the following attributions:

- to approve the Regulations on the Organization and Operation of the Body of Expert Accountants and Licensed Accountants in Romania, the modifications and the completions thereof, advised by the Ministry of Finance and by the Ministry of Justice, as

well as the Code of Ethics and Professional Behaviour of professional expert accountants and licensed accountants.

- to establish the basic guiding lines meant to ensure a good practice of the expert accountant and licensed accountant profession.

- to examine and approve, by open voting, the report of activity presented by the Superior Council for the expired financial period and the internal auditors' report on the financial management of the Superior Council.

- to approve, by open voting, the execution of the budget of revenues and expenses of the completed financial period, as well as the budget of revenues and expenses of the future financial period, presented by the Superior Council.

- to approve, by open voting, the organization chart of the Superior Council, the waging system for the year to come, as well as the principles and criteria of organization and waging of the own personnel and of that of the councils of the branches.

- at the proposal of the President of the Superior Council, to approve, by open voting, the system of granting and the quantum of the visiting and representation expenses within the branches of the Body for the year to come.

- to elect and to revoke the President and the members of the Superior Council and of the auditors' commission thereof, to elect and to revoke the president and two members of the Superior Commission of Discipline.

- to approve the report of the Superior Council on the results of the elections regarding the renewal of the members' mandate in the councils of the Body branches, revoking the elected persons being included.

- to approve, by open voting, the level of the indemnities for the elected boards of the Body and of the registration with the Body.

- to decide upon the proposals of disciplinary sanctions of the members of the Superior Council and of those of the councils of the branches, formulated by the Superior Discipline Commission.

- to decide annually the fees on revenue transhes, due by the members of the Body.

- to approve the annual plans of action of the Superior Council and of the councils of the Body.

- to confirm the list consisting of the honourable members of the Body, in conformity with annex no. 3.

- to establish the necessary steps and to follow up the fulfilment of any other task provided for in the norm acts, as well as in the own decisions.

The Superior Council exerts the rights of the Body afferent to its status of legal entity of public utility. It essentially has as an attribution the representation in front of the public authorities by means of its President and by means of the coordination of the activities of the councils of the county branches.

V. The *Authority* for State *Assets* Recovery ("AVAS")

The ***Authority for State Assets Recovery*** ("AVAS") is organized as a specialized institution with legal status of the central public administration, and subordinated to the Government.

AVAS's aims for the recovery of bad banking assets taken over from the majority State-owned company, in view of preparing them for privatization and reducing the State's financial effort in such operations. In view of reaching its goals, AVAS's main powers focus on taking-over, recovering and managing companies assets and debts associated with the same. The receivables titles and their accessories assigned to AVAS are executory titles, just like any other deeds or instruments entered by the latter for the recovery of company receivables. AVAS may organize its division of officers to act solely for the enforcement of such executory titles.

Any litigation involving AVAS in relation to bad companies debts taken over will be settled based on the observance of the special rules provided for by Government Emergency Ordinance no. 51/1998 (short judgment terms, special forced execution procedures etc.), accordingly completed by the provisions of the Civil Procedure Code. Additionally, the requests formulated by AVAS and any other procedural acts performed by and on behalf of AVAB in connection with companies assets recovery are exempted from stamp fees and taxes.

VI. The National Union for Public Notaries

The ***National Union for Public Notaries*** is a professional with legal personality organization, with a leading council and other bodies established with his own statute.

The Council of the Union is set up by one representative of each Chamber of the Public Notaries, from which will be elected one president and two vice-presidents.

The Council of the Union has the main following attributions:

- makes the proposal to the Ministry of Justice for decision of suspension, for revocation or ending of the function of public notaries;
- makes the proposal to the Ministry of Justice for the necessary number of the offices of public notaries and the conditions for the public notaries exams;
- establishes with the approval of Ministry of Justice, minimal wages for the public notaries;
- represents the public notaries on international and intern level in the relations with third parties;
- accomplishes all other attributions according to the regulations in the field.

VII. The National Union for Real Estate Agency (UNAI),

The ***National Union for Real Estate Agency (UNAI)***, established by Government Decision no. 3/21.012000, is a non-profit professional organization who have the main objective to regulate the activity in the field of real estate and for the rising of the professional prestige for the operating agencies in the field of real estate.

National Union for Real Estate Agency has the role to focus to the general interest of the real estate agents, in order to develop the real estate market, to become a real partner for the governmental institutions or non-governmental national and international institutions.

One of the major goals of the Union is to realize a better image of the real estate agents in front of the clients, partners, non-governmental organizations and state's institutions.

U.N.A.I. is involved in development of a healthy and active business field by:

- creation of a strong infrastructure;
- establishment of highest educational and professional standards;
- imposing and supervising the conformity with the legislation in the field of real estate;
- establishing the rules of functioning and operating standards of the agents of real estate.

UNAI is member of the Chamber of Commerce and Industry of Romania and the National Council of Small and Medium Sized Private Enterprises in Romania.

On international level the Union establishes relations with real estate organizations from Europe: Central European Real Estate Association Network (CEREAN) and from USA - National Association of Realtors (NAR) and it is associate member of CEPI (European Council of Real Estate Profession).

VIII. The National Association of Romanian Bars

All the lawyers from the bars form the ***National Association of the Romanian Bars*** that has the headquarters in Bucharest. None of the bar can function outside of the Association.

The Permanent Commission of the National Association of Romanian Bars ensures the permanent activity of the Association.

Its main attributions refer to:

- draws up the drafts of the statute and of the regulations for examining candidates for entering in profession order and for the final examination;
- organizes the exams for entering into profession and for the final examination;
- grants the exemption from examination to the legal advisers that accomplish the provisions of the law to become lawyer, having the decision of the bar council;
- organizes general statistics service of the lawyers;
- organizes, by the requests of the bars, courses and edits the publication of the Association;
- sets up the Central Credit and Aid for the Lawyers Unit and coordinates its activity;
- accepts donations made in favour to the Association;
- hires the personnel and ensures the budgetary execution;
- elaborates the annual activity report and submits it to the Council approval.

ANNEX 5

Legislation

INTERNATIONAL CONVENTIONS

- **United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances – 1988, Vienna**

Key Provisions:

•Criminalize laundering - Art. §1(b)
•Identify & trace proceeds of crime - Art. 5 §2
•Freeze and seize - Art. 5 §2
•Financial records - Art. 5 §3
•Override banking secrecy - Art. 5 §3
•Mutual legal assistance [Article 5, §4]
•Sharing confiscated assets [Article 5, §5(b)]
•Reversing onus of proof [Article 5, §7]

- **Council of Europe Convention no. 141 on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime – Strasbourg, 8 November 1990**

Key Provisions:

• Money laundering occurs also if the predicate offence is committed abroad;
• Negligent money laundering (not mandatory);
• Strengthening of the confiscation and provisional measures;
• Judicial co-operation and technical assistance.

United Nations Convention on Transnational Organized Crime – 2000 Palermo (not yet in force)

Key provisions:

•Shall include as predicate offences, all serious crime
• Shall institute regulatory regime for banks, non-bank financial institutions and other susceptible bodies
•Regime shall include
–Customer identification
–Record Keeping
–Reporting of suspicious transactions
•Authorities should have ability to cooperate and share information at national and international levels

EUROPEAN COMMUNITY

- **Council Directive on Prevention of the Use of the Financial System for the Prevention of Money Laundering – 91/308/EEC** – Brussels, 10 June 1991 - amended by
- **Council Directive on Prevention of the Use of the Financial System for the Prevention of Money Laundering – 2001/97/EC** – Brussels, 4 December 2001;

Definition of money laundering (art. 1):

'Money laundering' means the following conduct when committed intentionally:
- 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;
- 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;
- 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;
- participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counseling the commission of any of the actions mentioned in the foregoing indents.
Knowledge, intent or purpose required as an element of the above-mentioned activities may be inferred from objective factual circumstances.
Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.

FINANCIAL ACTION TASK FORCE:

• The Forty Recommendations;
• Special Recommendations on Terrorist Financing.

BASEL COMMITTEE ON BANKING SUPERVISION:

• Customer due diligence for banks, October 2001

ROMANIAN ANTI-MONEY LAUNDERING LEGISLATION:

• Law no. 656/2002 for the prevention and sanctioning of money laundering;
• Government Decision no. 479/16.05.2002 on the Regulations on Organizing and - Operating of the National Office for Preventing and Combating Money Laundering;
• Decision no. 762/2003 for modifying the Regulations on Organizing and - Operating of the National Office for Preventing and Combating Money Laundering;
• Decision no. 1078/2004 for modifying the Regulations on Organizing and - Operating of the National Office for Preventing and Combating Money Laundering;
• Decision no.657/2002 regarding the form and containing of the Report on suspect transactions, of the Report regarding operations with amounts in cash exceeding the equivalent of Euro 10.000, and of the Report regarding external transfers of amounts exceeding the equivalent of Euro 10.000;
• Law no. 78/2000 on the Prevention, Finding and Punishing of the Corruption Deeds in Romania;
• Romanian Penal Code – art. 118 – special confiscation;
• Romanian Penal Procedure Code - art. 163 – provisional measures.
• National Bank's Norm no.3/2002 regarding "Know-Your-Customer" (KYC) standards;
• Banking Law no. 58/1998;
• Law no. 143/2000 on the Combating of Drug Trafficking and Illicit Drug Consumption;
• National Commission for Securities' Order no. 25/1999 approving Instructions no. 9/1999 on the Prevention and Fight against Money Laundering;
• Law no. 263/15 May 2002 concerning the ratification of the Strasbourg Convention no. 141/1990 on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime;
• Law 39/2003 concerning the prevention and combating of organized criminality.

OPERATIONAL GUIDELINES FOR FINANCIAL INSTITUTIONS

- Phare Project RO02-IB/JH-08 – Suspicious Transaction Guidelines – Updated Edition Sept 2004.

ANNEX 6

WEB SITES

International institutions involved in AML - CTF

www.europa.eu.int
www.coe.int
www.fatf-gafi.org
www.imolin.org
www.interpol.int

National FIUS/Regulators

Albania - Central Bank
http://www.bankofalbania.org/

Algeria - Central Bank
http://www.bank-of-algeria.dz/

Argentina - Unidad de Información Financiera
http://www.uif.gov.ar/

Armenia - Central Bank
http://www.cba.am/

Aruba - Centrale Bank van Aruba
http://www.cbaruba.org/

Australian Prudential and Regulation Authority
http://www.apra.gov.au/home.cfm

Australian Transaction Reports & Analysis Centre (Austrac)
http://www.austrac.gov.au/

Bahamas Compliance Commission
http://www.bahamas.gov.bs/compliancecommission

Bahrain Monetary Authority
http://www.bma.gov.bh/

Bermuda Monetary Authority
http://www.bma.bm/

Belgium Banking and Finance Commission
http://www.cbfa.be/

Bulgarian National Bank
http://www.bnb.bg/

Brazil - Conselho de Controle de Altivades Financeiras
http://www.fazenda.gov.br/coaf/

British Virgin Islands Financial Services Commission
http://www.bvifsc.vg/

Canada Office of the Superintendent of Financial Institutions
http://www.osfi-bsif.gc.ca/eng/default.asp

Carribean Development Bank
http://www.caribank.org/

Cayman Islands Monetary Authority
http://www.cimoney.com.ky/

Chile - Superintedencia de Valores y Seguros de Chile
http://www.svs.cl/sitio/index.html

Colombia - Unidad Administrativa Especial de Información y Análisis Financiero
http://www.uiaf.gov.co/Nuevo/index.asp?id=79

Committee of European Securities Regulators
http://www.cesr-eu.org/

Commonwealth of Dominica International Business Unit
http://www.ibuoffshoredominica.dm/

Cyprus Central Bank
http://www.centralbank.gov.cy/nqcontent.cfm?a_id=1

Eastern Caribbean Central Bank
http://www.eccb-centralbank.org/index.asp

Eastern Caribbean Securities Regulatory Commission
http://www.ecsrc.com/

Finland Financial Supervision Authority
http://www.rata.bof.fi/english/index.asp

Germany - Bundesanstalt für Finanzdienstleistungsaufsicht
http://www.bafin.de/cgi-bin/bafin.pl

General Insurance Standards Council, UK
http://www.gisc.co.uk/

Gibraltar Financial Services Commission
http://www.fsc.gi/fsc/home.htm

Grenada International Financial Services Authority
http://www.gifsa-grenada.com/

Guernsey Financial Services Commission
http://www.gfsc.guernseyci.com/

Hong Kong Monetary Authority
http://www.info.gov.hk/hkma/index.htm

Hungarian Financial Supervisory Authority
http://www.pszaf.hu/

Iran - Central Bank of Iran
http://www.cbi.ir/e/

Irish Financial Services Regulatory Authority
http://www.ifsra.ie/

Isle of Man Financial Supervision Commission
http://www.fsc.gov.im/

Japan Financial Services Agency
http://www.fsa.go.jp/indexe.html

Jersey Financial Services Commission
http://www.jerseyfsc.org/

Korea Financial Supervisory Service
http://english.fss.or.kr/en/englishIndex.jsp

Labuan Offshore Financial Services Authority
http://www.lofsa.gov.my/lofsa5/index.htm

Luxembourg Commission du Surveillance du Secteur Financier
http://www.cssf.lu/fr/index.html

Malta Financial Services Authority
http://www.mfsc.com.mt/mfsa/index.htm

Mauritius Financial Services Commission
http://www.fscmauritius.org

Monetary Authority of Macau
http://www.amcm.gov.mo/

Montserrat Financial Services Commission
http://www.fscmontserrat.org/

Nevis Financial Services
http://www.nevisweb.kn/about.cfm

Nigerian Economic and Financial Crimes Commission
http://www.efccnigeria.org/

Peru - Central Reserve Bank
http://www.bcrp.gob.pe/English/Index_eng.htm

Peru - Superintendencia de Banca y Seguros
http://www.sbs.gob.pe/PortalSBS/

Puerto Rico Office of the Commissioner of Financial Institutions
http://www.cif.gov.pr/html/message.html

Saudi Arabian Monetary Agency
http://www.sama.gov.sa/indexe.htm

Singapore Monetary Authority
http://www.mas.gov.sg/

St Vincent and the Grenadines Offshore Finance Authority
http://www.stvincentoffshore.com/index.htm

Swiss Federal Banking Commission
http://www.ebk.admin.ch/

Swiss Federal Finance Administration
http://www.gwg.admin.ch/e/index.htm

Thailand Anti Money Laundering Office
http://www.amlo.go.th/

UK Financial Services Authority
http://www.fsa.gov.uk/

US Securites and Exchange Commission
http://www.sec.gov/

Venezuela - Superintendencia de Bancos y Otras Instituciones Financieras
http://www.sudeban.gov.ve/sudeban/main.jsp