Financial Action Task Force on Money Laundering

Groupe d'action financière sur le blanchiment de capitaux

Report on Money Laundering Typologies 2002-2003

14 February 2003

FATF Secretariat
2, rue André-Pascal
75775 Paris Cedex 16
FRANCE

Contact@fatf-gafi.org

TY2003_en.doc
03.03.2003//16h00

TABLE OF CONTENTS

LIST OF CASE EXAMPLES

INTRODUCTION

1. The threat to the financial system posed by money laundering and terrorist financing remains very real. The anti-money laundering effort has been a cornerstone of the fight against serious crime on a global level since the late 1980s. The fundamental objective of this effort is to ensure that criminal misuse of the financial system is detected and defeated. Confronting terrorist financing has taken on new urgency since the terrorist attacks in 2001. Indeed, during the past year, terrorist groups have shown their ruthlessness in high visibility attacks in Tunisia, Bali, Pakistan, Russia, and Kenya. More than likely, all of these incidents will have been supported by some sort infrastructure that would have had to use some part of the international financial system. Money laundering is an evolving activity, and we are still trying to learn more about the concrete methods terrorists use for getting the funds they need to where they need them. Consequently, both of these phenomena must be examined on a continuing basis to ensure that counter-measures can be both timely and effective.

2. The Financial Action Task Force (FATF) uses its annual typologies exercise to monitor changes and better understand the underlying mechanisms of money laundering and terrorist financing. It does this with the objective of being able to report on some of the key methods and trends in these areas and also to ensure that the FATF Forty Recommendations and Eight Special Recommendations remain effective and relevant. This year's meeting of experts on money laundering and terrorist financing took place on 19 and 20 November 2002 in Rome, Italy. Under the chairmanship of Dr. Carlo Santini, Director General of the *Ufficio Italiano dei Cambi*, 35 countries and jurisdictions came together for this year's meeting of experts, including representatives from FATF members: Argentina; Belgium; Brazil; Canada; Denmark; the European Commission; Finland; France; Germany; Greece; the Gulf Co-operation Council; Hong Kong, China; Ireland; Italy; Japan; Luxembourg; Mexico; the Kingdom of the Netherlands; Norway; Portugal; Singapore; Spain; Sweden; Switzerland; Turkey; the United Kingdom; and the United States; as well as the two new FATF observer members, the Russian Federation and South Africa.

3. Also present at the meeting were representatives of the FATF-style regional bodies: the Asia Pacific Group on money laundering (APG, with representatives from Korea and Pakistan), the Caribbean Financial Action Task Force (CFATF, with representatives from the Bahamas, Panama, and Trinidad & Tobago), the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), the Financial Action Task Force on Money Laundering in South America (GAFISUD), and the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL, with a representative from Hungary). The following observer organisations also sent representatives: the Egmont Group of financial intelligence units (with representatives from Monaco and Romania), the International Monetary Fund (IMF), the International Organisation of Securities Commissions (IOSCO), Interpol, and the World Bank.

4. Earlier in 2002, the FATF agreed to a series of topics or themes for this year's exercise. These topics included the role of non-profit organisations and informal money or value transfer systems in terrorist financing, money laundering vulnerabilities in the securities sector, and the potential risks in the markets for precious metals and gems, with a particular emphasis on gold and diamond trading. Written material produced by the FATF delegations and invited experts was collected and circulated prior to the meeting and provided the starting point for debates on each topic. Also as part of the typologies exercise for this year, FATF members submitted money laundering statistics and information on other relevant trends, as well as examples of money laundering indicators.[1]

---

[1] The material collected for this last item will be used in producing guidance on detecting suspicious transactions related to money laundering. The FATF will publish this guidance later in 2003.

5. This report on the FATF-XIV typologies exercise incorporates some of the key findings made during the meeting of experts with the written material circulated beforehand. It is divided into chapters on each of the major topics described in the paragraph above. As is the usual practice of the FATF, the report includes case examples taken from the written contributions and presentations made during the meeting. The texts of these examples are reproduced here – wherever possible – as they were submitted for the exercise. However, country names, currencies and some other details have been modified in order to protect sensitive details of specific investigations.

CHAPTER 1: TERRORIST FINANCING

General Considerations

6. Last year's FATF Typologies report made a distinction between "fundraising" or the collection of funds and the "laundering" or processing of those funds. This distinction is taken up again in this year's report as a means of providing a context for the discussion of the misuse of non-profit organisations and the informal transfer systems by terrorist organisations.

7. Experts believe that the two principal sources of funding for terrorist groups are from illegal and legal revenue generating activities. Terrorist groups may derive income from criminal acts in much the same way that organised crime groups do. One group given as an example both in previous and current typologies exercises derives the bulk of its capital from kidnapping (demanding ransoms) and extortion (of so-called "revolutionary tax" or protection money) in the area that it operates. Another group, also mentioned in previous exercises, uses funds obtained through narcotics trafficking for the bulk of its income. In obtaining funds from illegal activities, the actions of the terrorist group do not differ from those of a non-terrorist criminal organisation.

8. Unlike other criminal organisations, however, terrorist groups may also rely on apparently legal sources of income. Such methods as solicitation of donations, sales of publications, collection of membership dues or subscriptions, and charging fees for cultural or social events are all examples of legitimate sources of funding that may be used by terrorist groups. In some instances, these individual donors may not be aware that their contributions are being used by terrorist groups. In other cases, however, it may be that the donors are aware of the ultimate use that their donations will serve.

9. While terrorist groups may support themselves with funding from illicit and legitimate sources, they "process" these funds – that is, move them from the source to where they will be used – in much the same way that non-terrorist criminal groups launder funds. The FATF experts continue to find that there is little difference in the methods used by terrorist groups or criminal organisations in attempting to hide or obscure the link between the source of the funds and their eventual destination or purpose. One member indicated the following series of techniques and mechanisms that had been detected in relation to terrorist financial activity in his country:

- Front Companies – companies which actually carry on business where illegal profits can be co-mingled with revenues derived from legitimate undertakings.

- Shell Companies – businesses without substance or commercial purpose and incorporated to conceal the true beneficial ownership of business accounts and assets owned.

- Informal Money or Value Transfer Systems – funds transfer systems provided through such systems as *hawala*[2], *hundi*, *fei-chien* and the *black market peso exchange*.

- Nominees – use of family, friends or associates who are trusted within the community, and who will not attract attention, to conduct transactions on their behalf to disguise the source and ownership of funds.

- Structuring (smurfing) – depositing of cash or purchasing of bank drafts at various institutions by several individuals, or the carrying out of transactions below reporting thresholds.

[2] In Arabic, the term *hawala* means "transfer". In this document however, the term *hawala* refers to a type of informal transfer system.

- Credit Cards (front-end loaded) – creating credit on a card by paying cash on the card allowing the credit to be converted to cash.

- Electronic Funds Transfer – use of wire transfers services to transfer funds to associates.

- Currency Smuggling – the physical movement of cash from one location to another to disguise its source and ownership.

10. When looking at the individual steps that might be taken to move or dissimulate funds – wire transfers, commingling with legitimate monies, set up of non-transparent legal entities, transfers through informal money or value transfer systems, etc. – it would be difficult if not impossible to determine by the activity alone whether the particular act was related to terrorism or to organised crime. For this reason, these activities must be examined in context with other factors in order to determine a terrorist financing connection.[3]

Misuse of Non-Profit Organisations in Support of Terrorist Financing

11. In previous FATF typologies exercises, experts have discussed the potential misuse of non-profit or charitable organisations in support of terrorist fundraising. While it was clear that some non-profit organisations (NPOs) had played a role in terrorist financing in the past, the extent and nature of this role were not clear. From the examples examined in last year's exercise, it appeared that this role was either as a means of raising funds for terrorist groups and / or serving as a cover for moving funds in support of such activity. Material from this year's exercise, as discussed later in this report, appears to confirm this finding.

12. The voluntary or charitable sector can be described as one of key providers of certain services to society, together with the public and private sectors. Non-profit and charitable organisations, associations and foundations touch almost all aspects of life including education, health, religion, human rights, social justice, humanitarian causes, environment, the arts, culture, sports and recreation. In many countries, they provide essential services, which take such forms as neighbourhood associations, service clubs, advocacy coalitions, food banks, homeless shelters, drug and alcohol rehabilitation programmes, museums, sports clubs, and religious organisations.

13. NPOs are established in a wide variety of legal forms and are subject to varying degrees of control by the jurisdictions in which they are located. Given the diversity of NPO forms and relevant oversight systems, the FATF has adopted a definition of NPOs which is based on their function rather than on their legal form. The term NPO is therefore used with the meaning of any legal entity that engages in the raising or disbursing of funds for charitable, religious, cultural, educational, social, fraternal, or humanitarian purposes, or for the purposes of carrying out some other type of "good works".[4]

14. The potential misuse of NPOs by terrorist groups can take many forms. One possibility is the establishment of an NPO with a stated charitable purpose but which actually exists only to channel funds to the terrorist organisation. Another possibility is that an NPO with a legitimate humanitarian or charitable purpose is be infiltrated by terrorists or their supporters. Once in key positions within the

[3] For a more complete discussion on terrorist financing indicators, see *Guidance for Financial Institutions in Detecting Terrorist Financing* (24 April 2002), available on the FATF website at: http://www.fatf-gafi.org/TerFinance_en.htm. Additional guidance on money laundering indicators will be published later in 2003

[4] For further discussion on this topic, see *Combating the Abuse of Non-Profit Organisations* (11 October 2002), available on the FATF website at: http://www.fatf-gafi.org/TerFinance_en.htm.

organisation, some of the funds collected for ostensibly legitimate charitable causes can be diverted to direct or indirect support of the terrorist organisation. In this latter case, it is often without the direct knowledge of the donors and, in some cases, members of the staff and management of the NPO itself. Still another possibility is for the organisation to serve as an intermediary or cover for the movement of funds – usually on an international basis. In some cases, the NPO support function could also extend to the movement and logistical support of the terrorists themselves.

Example 1: Misuse of a position within an NPO and unwitting donors

Non-profit organisation P had branch offices in different countries where it had co-operative development projects. Individuals associated with a terrorist organisation ran some of these branches. Organisation P was however unaware that key persons working in its offices in Country X had connections with this terrorist organisation.

Organisation P had a headquarters in Country X, and one of its offices was located in a beneficiary country (Country Y). Despite the fact that Mr. B, the person in charge of Organisation P in Country Y, was not included in the employees' roll in Country X, he nevertheless received donations from different people and international bodies. Mr. B diverted those funds to a terrorist organisation, taking advantage of his position and anonymity in Country X.

This activity was made easier because the project was financed by donors who were unaware of the total amount of money involved. It was therefore possible to maintain an unjustified amount of money. In addition, since the projects were carried out in very remote areas, there was some delay before the beneficiaries discovered that they had only received a small amount of money. The investigation was difficult because the donors were also responsible for verifying the carrying out of the project. In this case, because the donors were certain public sector organisations, the checks were never performed.

Example 2: NPO used as part of a network of organisations for channelling terrorist funds

The financial intelligence unit (FIU) in Country Z received a report from a bank about non-profit organisation A with its registered office in Country Z which held accounts with the bank. The accounts held by Organisation A regularly received cash deposits and international money transfers from another non-profit organisation (Organisation B). These funds were then transferred abroad.

The bank's suspicions were first aroused by a newspaper article in which the name of Organisation B was mentioned as being suspected of having links with the 9/11 terrorist attacks in the US. The article mentioned the existence of links in Country Z with Organisation A and with one of its founding members. After checking its files, the bank found that Organisation A and the founding member in question held accounts at one of its branches.

Police information obtained by the FIU showed that the accounts of Organisation B had been blocked in connection with the enquiry into the 9/11 terrorist attacks. It also emerged that Organisation A and its founders were known to foreign police forces in connection with enquiries into groups suspected of links to the Al-Qaida network, one of the organisation's founders also having been arrested in connection with 9/11.

The FIU's analysis showed that Organisation B was active in Country Z as an intermediary for Organisation A. The funds transferred from abroad to the account of Organisation A on the instructions of Organisation B as well as the cash deposits were then transferred abroad to the accounts of other non-profit organisations. In the light of these elements, the transactions on the accounts of Organisation A may have been linked to the financing of terrorist activities. Consequently the FIU transferred this file to the public prosecutor's office, which initiated an investigation.

Recently the names of the Organisations A and B appeared in the *US Executive Order 13224 on terrorist financing*. The competent authorities also forwarded these names to be added to the consolidated list under UN Security Council Resolution 1267 (1999) for the freezing of assets.

Difficulties in detecting misuse of NPOs

15. FATF experts highlighted the difficulties in detecting misuse of NPOs by terrorist organisations. In certain instances, the connection between an apparently suspicious financial activity and terrorist financing was determined because the persons or entities involved – or linked to the NPO in some other way – were included in the UN Security Council Resolution lists of persons and entities associated with terrorism.[5] After establishing an alleged terrorist connection through the lists the authorities must then conduct their own financial investigations and attempt to obtain additional information from abroad.

16. Internationally, the variety and the different standards of professional record keeping and accounting procedures used within NPOs – especially from jurisdiction to jurisdiction – make the identification of potential "rogue transactions" very difficult. The concept of regular alms giving in certain cultures means that there are a large number of legitimate small donations to some charities, thus further complicating investigations into potential abuse. Furthermore, as terrorists learn the methods used by law enforcement and the regulatory bodies to discover misuse, their sophistication in disguising illicit funds will increase, making detection more difficult.

Counter-measures

17. One of the Special Recommendations issued by the FATF in October 2001 (SR VIII) specifically addresses the issue of NPOs. It proposes that countries take steps to ensure that NPOs cannot be misused by terrorists to finance their activities. During the past year, the FATF has worked on developing additional guidance for SR VIII. In October 2002, it published a best practices document[6], which offers concrete examples of actions that can be taken to ensure that NPOs are not co-opted by terrorists.

Informal Money or Value Transfer Systems and Terrorist Financing

18. Concerns have been raised from a number of sources that terrorist groups may be using channels outside of the traditional financial sector in order to move their funds. Since last year, a great deal of attention has been focused on the possibility that terrorist financing takes place through informal money or value transfer (IMVT) systems, particularly through hawala. This year, the FATF experts were asked to identify examples of such activity and attempt to show any links to terrorist financing.

What are "Informal Money or Value Transfer Systems"?

19. An informal money or value transfer system is one in which money is received for the purpose of making it or an equivalent value payable to a third party in another geographical location, whether or not in the same form. Such transfers generally take place outside of the conventional banking system through non-bank financial institutions or other business entities whose primary business activity may not be the transmission of money. The transactions of IMVT systems may sometimes

[5] UN Security Council Resolutions 1267 (1999) and 1390 (2002)

[6] See *Combating the Abuse of Non-Profit Organisations: International Best Practices*, (11 October 2002), available on the FATF website at: http://www.fatf-gafi.org/TerFinance_en.htm.

interconnect with formal banking systems (for example, through the use of bank accounts held by the IMVT operator). In some jurisdictions, IMVT systems are often referred to as *alternative remittance services* or *underground / parallel banking systems*[7]. Often there are ties between certain systems and particular geographic regions, and such systems are therefore also described using a variety of specific terms, including *hawala*, *hundi*, *fei-chien* and the *black market peso exchange*.

20. To transfer money through an IMVT, a customer presents funds to an IMVT operator[8] in his or her location and requests that they be transferred to an individual in another location. The IMVT operator receives the funds and then communicates with an IMVT operator at the transfer destination to request that funds be paid out to the individual identified by the initial customer. The communication may occur by telephone, facsimile or internet. The initial IMVT operator generally charges the customer a small fee or percentage of the transfer amount. While in some cases the two IMVT operators may work for the same business, generally the relationship between the two is simply based on trust and may be built on family, ethnic or linguistic ties, as well as business connections.

21. While in theory IMVT operations would tend to be balanced by funds being transferred in both directions, in practice the volume of transfers may be higher in one direction or the other. Consequently, IMVT operators need to "settle" their accounts. This may be done simply by transferring funds through the conventional banking system, physical shipment of currency, or else through one or a series of commercial or trade transactions.[9]

22. IMVT systems are in many countries an important means for transferring money. Indeed in some cases, they may be the sole reliable method available for getting funds to recipients in remote locations or those regions that do not have other types of financial services available. In more developed countries, IMVT systems often support immigrant populations desiring to repatriate earnings. Because these systems operate outside the conventional financial system, however, IMVT systems are also vulnerable to being used by criminals desiring to move funds without leaving an easily traceable paper trail. FATF experts have for years indicated IMVT systems as key facilitators of the movement of funds generated by criminal activity. Cases provided for this year's typologies exercise appear to confirm that IMVT systems continue to be exploited by criminals. The examples also show that it is often impossible to determine simply by the existence of an IMVT operation whether funds flowing through it are legitimate or not.

Example 3: Informal money or value transfer system supported by import/export activity

This case is derived from the statement of a suspect arrested on suspicion of illegally staying beyond the period of his visa in Country M. As a result of investigation, two suspicious bank accounts were identified. Approximately 1,100 individuals transferred a total of approximately USD 26 million to these two accounts.

In November 2001, a national from Country S was arrested in Country M on suspicion of unlicensed banking. The investigation revealed that this subject had been running an informal funds transfer system (*hawala*) for almost four years. Three other individuals, who had already left Country M, were also identified as associates. This group of IMVT operators settled the balance between Countries M and S through import/export transactions relating to car parts. The outline of their operation is described as follows :

[7] The FATF has dealt with this subject before (see the *FATF-XI Typologies Report* [3 February 2001], available through the FATF website at: http://www.fatf-gafi.org/FATDocs_en.htm#Trends).

[8] The IMVT operator is known as a *hawaladar* for transfers through *hawala*; IFT operators are known by other terms in other IMVT systems.

[9] For additional explanation of how IMVT systems work, see *The Hawala Alternative Remittance System and Its Role in Money Laundering* (January 2000) published by INTERPOL and *Informal Funds Transfer Systems: An Analysis of the Hawala System* (November 2002) produced by the International Monetary Fund and the World Bank.

1. A company exported car parts from Country M to an importer in Country S while charging a certain price (for example, USD 20,000)

2. The importer from Country S pays 50 percent of the price (USD 10,000) directly to the exporter in Country M.

3. The group of IMVT operators pays the other half of the price (USD 10,000) to the exporter in Country M.

4. In return, the importer in Country S pays 50 percent of the price (USD 10,000) to the group's account in Country S to settle the balance. The payment is made in local currency and at a rate advantageous to the receivers, so that the group makes a certain profit from this transaction.

It should be noted that the group of IMVT operators did not charge the customers a commission, which made this payment system even more attractive to the customers.

Links between IMVT systems and terrorist financing

23. Terrorist groups are believed by the FATF to use many of the same methods for moving or hiding their funds as those used by non-terrorist criminal organisations. This year, many FATF members reported uncovering cases in which IMVT systems had apparently been used for or had been created for the intention of supporting terrorist financing. The difficulty in detecting such activity is linked to the nature of IMVT systems themselves, that is, the fact that they operate outside the regulated financial sector.

24. Many jurisdictions have identified cases through suspicious transaction reports filed by financial institutions and which indicate that a particular business is involved in IMVT activity. Information linking any of this activity must then often rely on other sources such as other ongoing law enforcement investigations or intelligence information related to the individuals or businesses involved. According to one FATF member, IMVT systems increasingly utilise the mainstream banking system, particularly if they handle large amounts of cash. It would seem that the more often that IMVT operators use conventional financial institutions, the easier it would be to detect them. Nevertheless, there is still no easy way to obtain intelligence information that would show direct terrorist financing links.

25. In one example, IMVT activity was detected by a financial institution and reported through a suspicious transaction report. Further investigation proved that the monies involved were indeed part of an IMVT service that was providing support to terrorist groups. The key indicator for the financial institution in detecting the IMVT operation was that, although the business involved was small, its bank account had a turnover that was not commensurate with what one would expect for a business of its size and type. It should be noted that this could also be an indicator of involvement in the laundering of non-terrorist criminal funds. Only after further examination of other factors in this case was the link to terrorists determined.

Example 4: IMVT activity revealed through large turnover in small business account

Investigations were triggered by several reports of suspected money laundering filed by various banks over a period of three years in respect to a national of Country N born in South Asia. Although the suspect only ran a small business with an annual turnover of around USD 150,000, between USD 1.7 and USD 3.5 million a year flowed via his private accounts.

Investigations revealed that the suspect's business was the "headquarters" in Country N of an international "underground bank" with "branches" in several Central Asian and European countries. He had set up a "chain" in Country N numbering 14 "branches". In addition to small amounts intended to support relatives in the transferring parties' home countries, this illegal banking system was used to transfer considerable sums for human being smuggling into Europe.

In May 2000, the suspect and the manager of one "branch" of his system located in Country H, who was in Country N for a short while, were arrested. A number of properties were searched in an operation that took place throughout Country N. A writ of attachment for approximately USD 350,000 was issued against the suspect. Around USD 140,000 in cash was found in his safe and the money was confiscated in order to prepare the forfeiture. In addition, a debt-securing mortgage was registered for his house, which he had bought in cash for USD 400,000 shortly before his arrest.

The two accused persons, who admitted to the operation, have now been sentenced to imprisonment for violating provisions of Country N's legislation on foreign residents. The accused voluntarily renounced his claim to the confiscated cash amount of USD 140,000.

Example 5: IMVT service supports operations of a terrorist group

A recent successful money laundering investigation concerning a bureau de change operation uncovered evidence of the laundering of terrorist funds, derived from international smuggling. Certain similarities existed with the *hawala* system in that there were substantial cash payments into the bureau de change which were not reflected in its principal books and records nor were they reflected in the bureau de change's bank account. The bureau de change held a huge cash reserve which was drawn upon, when necessary by members of the terrorist organisation. In addition, the bureau de change would remit payments from its legitimate bank account to entities in other jurisdictions, on behalf of the terrorist organisation, which upon investigation was shown to be payment for contraband.

26. Several delegations noted a trend whereby there appears to be a link between specific NPOs and IMVT systems. Certain NPOs that disburse funds or provide assistance in some developing countries use IMVT systems to get necessary funds to remote locations or to areas that are not adequately served by traditional financial institutions. The observations made by the FATF experts appear to be something else. In one instance, the law enforcement authorities discovered that an NPO's headquarters was located in the same office as an IMVT service, which had already been linked to money laundering operations. The authorities in three other FATF member countries have observed the trend that certain IMVT services are avoiding new requirements to register or obtain a license by re-establishing themselves as NPOs. By avoiding registration as a money remitter, the supposed NPOs could then theoretically continue to remit money without having to submit to the oversight of the financial regulatory agency.

Example 6: NPO used as a cover for an IMVT service

The financial supervisory authority (FSA) of Country D has detected an increasing tendency for underground banking businesses with worldwide operating networks to try to circumvent the obligation to obtain a license by establishing themselves an incorporated association to serve as a cover for their illegal business of remittance services.

In several cases Country D's FSA shut down unauthorised remittance businesses. Later, however, the FSA found out that the same persons continued the business but had established and registered as associations for charitable purposes and hoped somehow to have placed their illegal business out of reach of the FSA. One typical example is the case of Association L for help in an African country (Country K) and with its headquarters in

Country D. It is part of an obviously worldwide operating network including for example offices in Europe, North America, the Pacific region and the Middle East. The pattern used is the same in all of the known cases as for the Association L case: The Country D branch of this association collected money from its principals and promised them to transfer and disburse the money to specified beneficiaries especially in Country K. Since its registration in mid-January 2002 until July 2002 Association A transferred approximately USD 500,000 before the office was closed down again.

Counter-measures

27. In this area as well, the FATF issued a Special Recommendation (SR VI) in October 2001. The intention of SR VI is to increase the transparency of alternative remittance (IMVT) systems vis-à-vis national authorities by attempting to bring them under some sort of oversight. Specifically, the Special Recommendation calls for, as a minimum, the licensing or registration of IMVT operators and the application of relevant FATF Recommendations dealing with the financial sector. The response from FATF members has varied. Some members have taken the approach that IMVT systems should be dealt with in exactly the same way as other funds remitters in that they should be licensed and / or registered and then subject to the same oversight procedures as conventional financial institutions. Others have simply established licensing or registration systems. The FATF is working on additional guidance on SR VI in the form of an interpretative note[10] and a best practices paper.[11] These documents will be published later in 2003.

28. One point that was emphasised by several experts is that IMVT systems provide a service that for the most part deals with funds from legitimate sources. While the need to increase the transparency of such systems is becoming almost universally recognised, including by jurisdictions outside the FATF[12], there is some concern that an overly restrictive approach may under certain circumstances have the opposite effect in pushing IMVT systems further underground. In addition, some experts in this area believe that solutions for dealing with IMVT systems must be found in the larger context of improving basic financial services infrastructure and regulatory / oversight regimes in those countries that are the primary receiving locations for IMVT operations.

[10] Published 14 February 2003 and available through the FATF web site at http:\\www.fatf-gafi.org.

[11] To be published later in 2003.

[12] See the *Abu Dhabi Declaration on Hawala* (16 May 2002).

CHAPTER 2: MONEY LAUNDERING THROUGH THE SECURITIES SECTOR

29. The FATF has attempted to examine the issue of money laundering through the securities sector before; however, it was hampered by the fact that there was little concrete information on how or if the markets were being used for such purposes. Indeed, although securities brokers have been covered by the obligation to make suspicious transaction reports for several years in some FATF members, the numbers of reports from the sector in general have not always corresponded to the relative size of the securities market. For this year's exercise, FATF experts were invited to look more closely for money laundering cases that were somehow related to the securities sector, whether through the misuse of various types of trading operations, the establishment of legal entities, or exploitation of various market mechanisms. The effort was successful in that many FATF members were able to locate relevant material based on money laundering cases or disclosures of suspicious transactions.

How can the securities market be used for money laundering?

30. The securities sector on a global scale is characterised by its diversity, the ease with which trading can now take place (through electronic trading for example), and the ability to perform transactions in markets with little regard to national borders. These characteristics make securities markets attractive to the ordinary investor looking for a good return on his or her money. These same characteristics, along with the sheer volume of transactions in many markets, also make the securities sector a potentially inviting mechanism for the laundering of funds from criminal sources.

31. The illegal funds laundered through the securities sector, according to FATF experts, may be generated by illegal activities both from outside and from within the sector. For illegal funds generated outside the sector, securities transactions or the creation of legal entities are used as the mechanism for concealing or obscuring the source of these funds. In the case of illegal activities carried out within the securities market itself – for example, embezzlement, insider trading, securities fraud, market manipulation, etc. – the securities transactions or manipulations generate illegal funds that must then be laundered. In both cases, the securities sector appear to offer the launderer the potential for a double advantage in allowing him to launder illegal funds and to acquire an additional profit from the related securities fraud.

Acceptance of cash and the entry of illegal funds into the securities sector

32. In many securities markets, only certain permitted persons or firms, such as stockbrokers, banks or certain independent financial advisors may perform transactions. These market operators are generally restricted or prohibited outright from accepting cash to carry out such transactions. Many of the FATF experts indicated that criminal funds in the form of cash must therefore be introduced into the financial system before entering the securities sector. Consequently, the use of the securities sector for laundering was considered by the experts to be primarily part of the layering and integration stages of money laundering.

33. Despite this view that the securities sector is unsuitable for the placement stage of laundering, a few cases provided by FATF members this year were examples in which a broker had accepted cash payments in violation of industry practice or formal rules against the practice. While the acceptance of cash likely represents the minority of laundering operations in most markets, the reliance on commissions as a source of income for securities market professionals – as was emphasised by more than one of the experts – can exert pressure to accept cash in violation of rules or procedures.

34. Given the size of the securities sector in some financial centres, it is reasoned by certain of the FATF experts that such markets could be a destination for large-scale criminal laundering. As mentioned above, to gain entry to the market, the launderer would require the assistance of a willing securities professional. With the financial resources available to organised crime groups, there is the inherent risk of corruption being used to gain entry to the sector. This means that illegal funds could enter the financial system through, for example, a co-opted professional service provider. As in other financial sectors, a further potential danger may be that some securities practitioners fail to comply with their customer du diligence obligations under the assumption that all customer due diligence obligations have already been performed by the financial institutions, professional service providers or other parties that send the funds to be invested.

35. Another way for illegal cash to enter the system is when certain types of securities trading operations are not covered by any cash acceptance restrictions. One FATF member described, for example, the difficulties encountered by its law enforcement and stockbrokers in dealing with the potential exploitation of margin trading for money laundering purposes. In an effort to turn a quick profit, settlement of trades in the margin trading market of the member's jurisdiction is often left until the last minute. Accordingly transfers and cheques are not used, as they take too long to clear, leaving cash as a popular settlement method. It is not uncommon for traders in the jurisdiction concerned to walk from one bank to another with large sums of money rather than use a bank draft in order to avoid handling charges. Settlement in cash makes it difficult for the broker to know for sure who is behind the deal. In these situations, the stockbrokers tend to assume that the banks receiving the cash have taken all steps to perform due diligence checks on customers and to make any necessary disclosures on transactions involving funds of suspicious origin. This type of settlement occurs in the markets of only a few countries.

Example 7: Stockbroker accepts criminal funds in cash

A stockbroker in Country C continuously accepted cash deposits from a client in the range of USD 7,000 to USD 18,000. The funds were placed in the money market fund of the client's sister and withdrawn through the issuance of cheques. After the broker was arrested on unrelated embezzlement charges, the client's identity became known to law enforcement. When the police conducted a background check on the client, it was revealed that the stockbroker's client was a known drug dealer.

Example 8: Cash criminal proceeds placed in the financial system through margin trading

This case involved the theft of some USD 384 million from a bank in Country T over the ten-year period from 1992 to 2001. The money was sent to Country G and laundered through a serious of companies and accounts (to date 80 companies and 550 bank accounts are involved, but this is growing as the investigation progresses). Much of the money was invested in the property and stock markets in Country G and ultimately used at will by the four principle thieves for whatever they wanted. At one time in the mid-nineties one of the thieves was reported as being the largest margin stock investor in the Country G market. There was a huge turnover in stocks and shares through some of Country G companies, as well as dividends from shares held long term. The true extent of the dealing is only just coming to light but it is evident that the majority of the funds stolen in Country T occurred after 1997 when a regional economic downturn adversely affected the local property and stock markets. It is of interest that no disclosures were ever made by stockbrokers about the dealings of these companies. At this time four people have been charged with money laundering and have been released on bail, and a number of other people are fugitives.

Layering of illegal funds

36. Another way to use the securities sector to launder illegal funds generated by non-securities related criminal activities is to purchase securities with illegal funds that have already been introduced into the financial system, that is, at the layering stage of laundering.

Example 9: Fraud money invested in securities market

A brokerage firm opened several accounts for a group of twelve linked individuals, including a non-resident account that was used to record very large movements and apparently to centralise most of the suspected flows, which totalled more than USD 18 million.

The launderers used the following two mechanisms:

- the accounts of some of the parties involved were credited with large sums received from countries of concern, which were invested in the stocks of listed companies in Country W; and

- the accounts of the individuals concerned were credited with sums from regions of concern, which were transferred to the non-resident account (the first accounts were used as screens).

This securities buy/sell mechanism was used to filter the flows through the broker and subsequently the clearer and custodian. Once filtered, the funds were sent to locations in regions of concern and offshore financial centres.

This information showed that the co-opted broker had been used to launder the proceeds from various forms of frauds. The manager of the brokerage firm served as a relay for the criminal organisations involved.

Setting up a company as a front for money laundering

37. In certain instances, mechanisms within the securities sector may be used for laundering funds regardless of whether their illegal origin is within or outside the securities sector. One such method is the establishment of a publicly traded company specifically to serve as a front for a money laundering operation. The typical example of such a scheme is for a criminal organisation to create a company for a legitimate commercial purpose and then to commingle illegal funds with funds generated by the legal commercial activity. Usually, the company would have to use various fraudulent accounting practices in order to succeed in such an operation. The establishment of various offshore entities through which funds may be channelled offers another way of obscuring the true intent of the operation. The advantage of using a publicly traded company for such a scheme is that its owners could profit twice from the mechanism: first in creating a successful means of laundering criminal funds and secondly in selling shares in the business to unwitting investors.

Example 10: Listed legal entity created specifically for laundering illegal funds

In 1994 a small eastern European enterprise was incorporated in Country A and started trading on a venture capital market. Company B supposedly manufactured magnets at its European subsidiary and was also in the business of trading oil to and from the former Soviet Union. During this period, the company was reporting tens of millions of dollars in sales and its year over year sales growth was double digit. The company's head office was located in Country C and in 1996, as a result of its dramatic growth, it met the listing requirements and its shares started trading on one of the stock exchanges of Country A.

The company was able to attract a high profile board of directors, including a former high ranking politician and was represented by a well-known established law firm. It had been identified that the founding shareholders of

the European enterprise were connected to an Eastern European organised crime group and whose interest in the company had been relinquished through a series of transaction in European and Caribbean "tax havens".

In the spring of 1997, Company B sought to raise an additional USD 74 million to make acquisitions and assist in the operations of the Company. The staff of the securities regulator agency in Country A became aware of "soft" intelligence that was impossible to confirm that raised concerns about the ongoing role of the Eastern European organised crime group in Company B. After an initial audit by a firm located in Country C, with the help of sub-audit by an accounting firm from the country of the European subsidiary, after a special review by a major international accounting firm of the original audit and after a new audit by a different major international accounting firm, all of which gave Company B a clean audit, the USD 74 million prospectus was receipted.

Four months after giving Company B a clean audit opinion, the auditors advised the company that they were extremely concerned about connections to organised crime and that many transactions may have been bogus. Eventually it was determined that the company was a front for laundering money and that:

–Sales were fictitious and bank accounts belonging to Company B were commingled with accounts belonging to entities controlled by the Eastern European crime group.

–Many sales transactions were conducted on a "cash" or barter basis.

–Assets were purchased from entities controlled by the Eastern European crime group valued at ten times their real value.

–Bogus sales commissions were paid to individuals belonging to the entities controlled by the Eastern European crime group.

–A Company B operating account was controlled by a member of the Eastern European crime group, and transactions involving millions of dollars went through the account.

–Company B engaged in transactions whereby suppliers of magnets, providers of goods and services, buyers of magnets and sellers of technologies were the same parties, that is, entities controlled by the Eastern European crime group.

–In respect to the USD 74 million offering, approximately USD 32.2 million was placed in an "unacceptable offshore bank" by an entity controlled by the Eastern European crime group.

In addition to laundering substantial sums of money for individuals and entities connected to the Eastern European crime group, original shareholders were able to sell their original shares on the open market and transfer the profits to Eastern European banks. At the end of the day, the original shareholders and their nominees profited from the sale of Company B stock in excess of USD 65 million.

In May of 1998, Company B's headquarters in Country C were raided by the police, and in the same month the securities regulatory agency in Country A halted trading of Company B shares. In November of 1999, the securities regulatory agency initiated proceedings in this matter. The hearing against the 13 respondents just finished and we are now awaiting the decision.

Market manipulation and money laundering

38. The term "pump and dump" is used by securities regulators and law enforcement authorities to describe the artificial inflation of a stock based on misleading information. This typical sort of securities fraud generates proceeds and is therefore a predicate offense for money laundering in most jurisdictions. In addition, there have been cases where this type of securities fraud has been set up

with the proceeds of other crimes, and sometimes money laundering can be used to advance this fraud. In a "pump and dump" scheme, individuals obtain large blocks of stock in a company before it is publicly traded or while it is dormant or not yet operational. A money launderer may use proceeds to purchase these large blocks of stocks. The shares are usually obtained at an extremely low price. After the perpetrators have accumulated large stock holdings in the company, they may utilise unscrupulous brokers to promote the securities to their clients. At this point, the securities fraud begins. Misleading information is released to the public – including in one example through the Internet – to promote the company and its business operations. Often, the company is misrepresented as having a revolutionary new product that will lead to future business success. As this false information is circulated, the share prices for the company rise due to public interest and increased demand. In the typical operation, the company has no legitimate operation and the information given to the public is simply provided to inflate the price of the shares. In order to create the appearance of market demand, the perpetrators of securities fraud may divide transactions among several brokers and / or channel transactions through multiple jurisdictions. When the shares reach a peak price, the perpetrators of this securities fraud sell off their share holdings and obtain a profit from the artificial inflation of the price. Eventually, the company is permitted to fail and the shares become worthless. At this point, two events have occurred: (1) the money launderer, by selling his stock in the company, has layered the illicit funds he originally invested; and (2) as a perpetrator of a securities fraud, he has generated additional illicit proceeds that require laundering.

Example 11: Market manipulation of company stock launders funds and produces added profit

The money in question came from a drug-trafficking organisation and was used to purchase two listed companies. During an investigation by the police of Country V into the laundering of money from drug trafficking, it was found that a money launderer had planned and executed a plan to feed large sums of money from a mafia-related organisation into the stock market. The money, which was the proceeds of various frauds, was deposited in a private bank, controlled by the mafia organisation itself, located in Country R located in the Caribbean region.

The plan included the purchase of two companies established in Country V and listed on the stock market. These were a stock brokerage and a small bank. The first stage took place as planned. Numerous small investors from abroad using false names bought the shares in the two firms. The aim was to ensure that none of the investors bought more than the percentage of ownership that would have required reporting under country V's laws.

Through fictitious general shareholders' meetings in which lawyers were involved, a new board of directors was appointed with people acting as front men for the money launderer, Mr. W. Upon gaining control of the two companies, Mr. W immediately granted full powers to the members of the criminal organisation, thus guaranteeing their control over the money.

Subsequently a share increase was applied for, and all the legal requirements were met. Again, they took care to ensure none of the investors exceeded the 5 percent limit. The share increase in the two companies came to approximately USD 42 million, which was subscribed and disbursed through banks in Country V. In reality the proceeds of the market manipulation, including the original funds, were then laundered by transferring the money from Country R to banks in Europe, from where it was transferred to Company N was located in Country Y, another offshore financial centre, and owned marble mines in South America. The money then returned to Country R, having first passed through accounts in Europe and North America. The same money then went around the circuit again, so as to simulate foreign investments in the share capital of the two companies.

Through this circular process of share buying and selling the price of the shares rose to 640 percent of their face value. To achieve this, the complicity of the brokers trading in the shares on the stock market was necessary. The over-priced shares were subsequently delivered to the mafia investors who were the final victims of the fraud when the police prevented the money launderer from controlling the price of the shares.

Example 12: Narcotics trafficker takes control of a publicly traded company

A drug dealer (Mr. D), a resident of Country A acquired the vast majority of freely tradable shares of ABC Ltd a public company with its head office in Country A. ABC Ltd was a speculative stock that traded on the over the counter market in Country B.

Mr. D sold drugs to Buyer A. He did not receive money. Instead, he instructed Buyer A to buy ABC Ltd through the stock market. Buyer A had previously set up an account in a non-cooperative jurisdiction and instructed his agent to purchase ABC Ltd. The agent contacted his broker in Country B and instructed him to purchase the shares. Mr. D instructed his agent in Country D to sell ABC Ltd. His agent instructed his broker in Country A to sell the securities. Because the stock was thinly traded there were not any competing bids for the security. The transaction was cleared through the clearing corporations with the end result being that Mr. D received the money and Buyer A received the drugs and the shares. Their cost was a few hundred dollars in commissions.

This transaction was repeated several times through several countries and brokers. It had the added benefit of providing liquidity to the market and the public was led to believe that there was actual interest in the security. The public then got involved in the trading and with the heightened awareness the stock increased in value. This meant that Mr. D and Buyer A's shares were now worth more and they were able to generate additional profits. Mr. D was able to legitimize the source of funds as being "market" profits.

39. As a related matter, the experts learned of one situation in which an individual allegedly paid another individual an inflated price for stock in order to pay criminal proceeds for a drug transaction. This both laundered the funds and began the securities fraud by creating the appearance of a market interest in the stock that influenced other, innocent investors.

Example 13: Placement in the stock of media sector companies

Several banking institutions of Country R reported to the FIU a series of transactions connected to the placement of shares representing the stock of a foreign company (Company D) listed on a major international exchange.

The transactions reported indicated a flow of funds from private investors located in Country R to another foreign company (Company E) operating in the media sector which transferred the money either to individuals linked in various ways with the company itself or to others seemingly acting as intermediaries for the placement of the shares. A reverse flow of cheques or other securities issued in the name of the two companies involved was also identified, but the instruments eventually turned out to be backed by insufficient funds or to be fraudulent.

Overall, an inflow of funds amounting to over USD 2.5 million was registered for the account of Company D, which was managing the placement of the stock over a one-year period.

In addition to the financial aspects of the activity, the financial investigation of the case performed by the FIU uncovered far more interesting indicators of the way the whole operation was structured.

A parent company of Company D was later incorporated in Country R. Its official activity ranged from the media sector, such as film production and the provision of Internet services, to estate investments, private hospitals and tourist facilities. Company D's stock was sold to investors in Country R and was indeed listed over the counter on the NASDAQ, but the value of the shares showed an extreme volatility, fluctuating from a minimum of USD 0.20 to a maximum of USD 24. Rumours of mergers with other companies or of major investments to be completed by the same Company D usually corresponded to the steepest surge in the value, only to turn out to be insubstantial at a later stage.

Most of the persons involved were allegedly registered stock brokers. Many of these individuals had connections with a brokerage house which in previous years had been implicated in serious irregularities and thus suspended

by the security regulator agency in Country R. Indeed, in many cases underwriters of the newly issued stock had been customers of that brokerage house and had purchased the securities by taking advantage of their previous positions. Most of the names of individuals involved were already known to the FIU through other suspicious transaction reports.

In conclusion, the whole operation was structured so as to lure unwary investors to invest in shares representing the stock of Company D, which, in actual fact, had no activity whatsoever. Due to the lack of depth in the market, the value of the stock seemed to be influenced by the release of false commercial information so as to provide the impression of easy capital gains. Company D used media concerns as a cover for its non-existent activities.

As a result of the suspicious transaction reports received by the FIU and because of the financial investigation it subsequently carried out, the financial supervisory agency requested the initiation of a criminal prosecution against those involved.

Example 14: Laundering related to securities law violations and possible link with terrorism

The FIU of Country L received an initial report from a casino regarding a Mr. N of foreign origin and residing in Western Europe who was purchasing gaming chips using various foreign currencies in large sums. Several similar reports from other casinos regarding the same individual were then followed up.

During the same period a bank made a report about one of its customers. The bank's suspicions had been aroused by the fact that this customer (Mr. K) was the principal shareholder of Company A, whose stock had been de-listed by a major stock exchange. Company A did not have an account with this bank, but Mr. K had signature authority on an account opened in the name of offshore Company B. This account was very active: several large transfers had been made from various companies in the goods haulage sector; these funds had then been transferred in particular to an account in a tax haven in the name of another party (Mr. E). Some time later, Mr. K approached a lawyer representing the offshore Company B to ask for a bank account to be opened in the name of a Company C incorporated under a foreign legal system, whose shareholders were Mr. K and the offshore Company B. The bank refused to open this account.

Company A, whose shares were quoted on a major stock exchange, was active in the transportation of second-hand vehicles from Europe to Africa. This company, operating via Country L, has its registered office in an offshore centre. Information gather by the FIU in Country L revealed that a stock exchange regulator had published an official notice announcing that the shares of Company A had been suspended pending an enquiry into fraudulent accounting practices at the company. These practices involved recourse to a network of offshore companies and consisted of intentionally spreading misleading information about its shares with the aim of manipulating the price. The stock market regulator has now begun a procedure to de-list this share.

From the FIU's analysis it appears that the parties appearing in this file used the financial system to conceal funds linked to stock exchange offences committed on the shares of Company A.

It appears that Mr. N, the beneficiary of the gift of several million dollars from Mr. K (principal shareholder of Company A) is the financial director of Company A. The latter had placed these funds in a share portfolio in his own name and had asked the bank if he could withdraw them in cash. The fact that the report from the bank was made before the funds were withdrawn in cash allowed the FIU to temporarily block the operation for 24 hours. This file was then urgently passed on to the public prosecutor to have seized the funds blocked following the Unit's intervention.

The involvement of an offshore company on whose account multiple transfers are made, especially when they are destined for a tax haven, and the request to open an account in the name of a company incorporated under foreign law of which the suspect persons are shareholders, are techniques designed to conceal the proceeds of crime and are frequently encountered in money laundering files.

The recourse to a legal professional is also a technique that is used by money launderers. It turned out incidentally that the lawyer involved in this file was already known to the police for his involvement in tax frauds carried out by means of debt-collecting agencies. Operations involving the purchase of gaming chips at casinos by Mr. N were also intended to conceal the proceeds of crime. The use of operations of this kind is a phenomenon that is also encountered in money laundering files.

Finally, information recently collected by the Unit revealed that Mr. E is also connected with Company A and is suspected by the judicial authorities of being involved in arms trafficking organised from an offshore centre where the registered office of Company A is located. What is more, there are suspicions regarding possible links between this arms trafficking and a terrorist network, the offshore centre in question being regarded as one of the bastions of this particular terrorist group.

40. FATF experts agreed that the securities sector possesses certain attributes that make it potentially vulnerable to being exploited by money launderers:

- The securities markets are not generally used for the placement stage of laundering. However, individual cases appear to show that the purchase of securities with illegally generated cash cannot be completely ruled out, even in jurisdictions that restrict or prohibit the acceptance of cash for such transactions.

- Because the industry relies on commissions for some of its operators, these professionals – whether individual brokers or employees of brokerage firms – may be tempted to ignore rules or regulations in order to ensure that a particular operation or client does not go to the competition.

- In some securities markets, due diligence procedures on customers or the source of their funds are not always performed in a consistent manner or do not go beyond the last step of the transaction. Some professionals assume that due diligence has already taken place, thus they may not to be as vigilant.

- The highly international nature of the securities industry means that launderers can use operations involving multiple jurisdictions to further complicate and thus obscure the various components of a laundering scheme. Again, when multiple jurisdictions are involved, securities professionals may erroneously assume that adequate due diligence procedures on a particular customer have already taken place in another jurisdiction. The experts stressed the importance of international co-operation in obtaining records to combat money laundering and the underlying predicate offences.

- As with transactions conducted through other parts of the financial system, ownership and control can often be hidden through the use of nominees, legal entities, trusts, etc.

41. FATF experts were generally of the opinion that current standards contained in the FATF Forty Recommendations were sufficient regarding the securities industry. However, these measures must be adequately and consistently applied to all securities markets and the professionals operating within them. At the same time there is perhaps a need to increase the awareness within the securities sector of the particular risks of money laundering that it faces. According to one FATF member, increased awareness would in turn cause more disclosures of suspicious transactions to be made.

CHAPTER 3: THE GOLD & DIAMOND MARKETS

42. In earlier typologies exercises[13], FATF members have made references to cases in which the trade in gold, precious metals and precious stones were exploited in some way for money laundering purposes. Illegal trade in diamonds has become an important factor in armed conflict in certain areas of the world, and terrorist groups may be using diamonds from these regions, according to the international press, to finance their activities. For all of these reasons, the FATF decided to take another look at this subject as part of this year's typologies exercise.

The Gold Market

43. Precious metals, and in particular gold, offer the advantage of having a high intrinsic value in a relatively compact form. Gold can be bought and sold for currency with little difficulty in most areas of the world. Furthermore, it holds its value regardless of the form it takes – whether, for example, in bullion or as a finished piece of jewellery – it is thus often sought after as a way of facilitating the transfer of wealth. For some societies, gold carries an important cultural or religious significance that adds to the demand for the metal in certain regions of the world.

44. The advantages that gold provides are also attractive to the money launderer, that is, the high intrinsic value, convertibility, and potential anonymity in transfers. It is used, according to the FATF experts, both as a source of illegal funds to be laundered (through smuggling or illegal trade in gold) and as an actual vehicle for laundering (through the outright purchase of gold with illegal funds). Most laundering involving gold are linked to illegal narcotics trafficking, organised crime activities and illegal trade in goods and merchandise. FATF members submitted a number of money laundering case examples, and some of the relevant typologies are described below. With regard to the use of the gold trade by terrorist groups, FATF members found certain indicators of terrorist connections; however, no concrete case studies were made available.

45. In the first and simplest typology, the money launderer or often someone acting on his behalf simply purchases gold from a retail merchant with funds that were generated directly by an illegal activity.

Example 15: Retail gold purchases serves as direct method of laundering

A foreign national used the services of a bureau de change to buy 265 ingots of gold with a total value of about USD 2,440,000, paid in cash. These transactions took place over a period of 18 months. The buyer, who did not have a bank account, alternated temporary jobs with periods of unemployment, suggesting that he was acting on behalf of a third party, whether a natural or legal person, who was probably involved in drug trafficking. The facts were forwarded to the prosecutor, and an investigation is ongoing.

46. The gold itself may be the "proceeds" of crime that needs to be laundered. In this case, the launderer may attempt to hide the illicit nature of the gold – for example, if it has been stolen or smuggled – by creating a system of false invoicing.

[13] In particular, the *FATF-IX Typologies Report* (12 February 1998) and the FATF-X Typologies Report (11 February 1999), both available on the FATF website at: http://www.fatf-gafi.org/FATDocs_en.htm#Trends.

Example 16: Gold purchases facilitate laundering

An asset management company was responsible for managing the bank portfolios of two individuals active in gold purchases in Africa. The purchased African gold was then sold to a gold working company in Country F, which in turn forwarded its payments to the accounts of the sellers.

Debits were regularly made from these accounts to accounts in another European country. Desiring to verify the use of the funds, the asset management company requested its clients to provide a description of the channels used for making the payments for the gold in Africa. The information received permitted the company to identify an intermediary residing in Europe who was responsible for paying the suppliers in Country F. The individual in question was described as being closely associated with a corrupt regime in Africa.

Based on this information, the asset management company reported the case to the FIU and proceeded to block the accounts. Information exchanged with foreign counterparts permitted the linking of this illegal trade with an ongoing foreign investigation, which targeted the same individual for arms trafficking. The case was transmitted to the office of the public prosecutor which is now working with the foreign authorities to dismantle these operations.

47. Another still more complex typology uses the gold or precious metal purchases and sales as a cover for the laundering operation. In certain instances, some of the supposed transactions of a particular scheme do not take place at all but are represented with false invoicing. The paperwork is then used to justify the transfer of funds to pay for these shipments. The false invoicing scheme is also common to the various value added tax fraud schemes, which are associated with certain gold trafficking operations.

Example 17: Gold processing company used as a cover for money laundering

The money laundering organisation used a company processing and working gold to introduce cash from the sale of cannabis in Country R into the banking system of Country P. Moreover, the money launderers used a system that had been designed to make payments relating to cigarette smuggling and defraud Country P by applying for value added tax (VAT) refunds for non-existent operations.

The organisation had a person operating in Country R who collected bags full of sterling and other European currencies at restaurants and hotels near airports. The money came from the sale of cannabis in various European countries. The money was transported by air to Country P and declared in customs as payment for gold the company in Country P had sold to a company in Country R.

The various currencies were paid into bank accounts in a city in Country P, certifying the origin of the money by means of the customs declaration completed at the border. These sales of gold by the company in Country P to the company in Country R were fictitious, although they were documented by false invoices. Subsequently the gold was supposedly sold to a company in a nearby offshore location, which issued a false letter of receipt.

The fictitious gold sales made it possible to transport money in cash from Country R to Country P where it was deposited in banks. Furthermore, it enabled the money launderers to apply for a refund on the VAT supposedly paid.

In order for this mechanism to work the money launderers operated a gold working company which bought gold ingots from the largest metal wholesaler in Country P. Part of the gold was used to manufacture gold wire and shipped to Country F, where it was delivered to a finishing company that melted it back down and sold it, paying by bank transfer to the same banks in Country P. Another portion of the gold sold by the company was diverted onto the black market where it was sold without VAT and therefore at an advantageous price for its buyers.

To complete the circuit, given that the initial gold purchase from the wholesaler had not been subject to VAT, the organisation set up a group of companies run by front men who issued false invoices for the sale of gold on which VAT was applied.

The system used also enabled the organisation to change funds into the local currency and introduce them into the banking system. This money was used to pay transport costs and bribes relating to cigarette smuggling. The vehicles travelled through Country P but never reached their cities of destination in the neighbouring region.

Example 18: Silver and gold smuggling

The investigation, conducted on the basis of official statements, of the examination of bank and company documentation pertaining to various juridical subjects obtained in the framework of several international rogatory commissions, as well as by carrying out appropriate judicial police activities (wiretaps, surveillances, searches, seizures, etc.), permitted the detection of a silver and gold smuggling system aimed at (1) introducing into Country J and other countries precious metals not subject to value added tax (VAT), (2) laundering illicit profits of criminal organisations (of local, regional and global scope) through banking and financial system channels to which the large movement of money was justified by the fictitious payment of precious metals supplies.

In particular, the way in which the laundering took place may be briefly outlined as follows:

1. Creation of a network of companies, including financial ones, throughout the region with the task of "filtering" the money.
2. Using the illicit proceeds of crime (derived from cigarette smuggling, drug trafficking, trafficking of weapons, smuggling of oil products) to purchase silver and gold that was, in turn, smuggled into the markets of Country J and other European countries.
3. Reinvestment of the profits of the illicit trafficking of silver in smuggling activities.
4. Use of false invoices in respect to the importation of precious metals (which never actually reached Country J), only for the reason of justifying the export of large amounts of illicit origin through the bank system.
5. Use of bearer savings deposit passbooks and of false Treasury certificates of deposit to be offered as guarantee to the banks for the purchase of precious metals.

As for the outcome of the investigation, it may be summarised as follows:

–15 subjects arrested for criminal conspiracy aimed at money laundering and smuggling.
–4 subjects accused of money laundering.
–Total amount of funds involved in the fraud was USD 101 million, with consequent evasion of duties for USD 72 million and VAT for USD 37 million; detection of money laundering for over USD 31 million.

The Diamond Market

48. Diamonds and other precious gems afford some of the advantages as those provided by gold – high intrinsic value in a compact form. Diamonds in particular can also be traded with little difficulty world-wide, although there is far more concentration for some aspects of the trade to certain regions. The large scale production of raw diamonds is limited to a few areas of the world – South Africa, western Africa, Australia, Canada and the Russian Far East to name just a few of these – and high-volume trading in diamonds is concentrated in a few locations – Antwerp, New York, Tel Aviv, for example. For these reasons, it appears that not every country or region will have the same level or type of diamond trading activity.

49. The ease with which diamonds can be hidden and transported and the very high value per gram for some stones make diamonds particularly vulnerable to illegal diversion from the legitimate

channels for the exploitation and profit of criminals. Security in all phases of the diamond industry is therefore a critical necessity in all phases of the diamond industry. One expert observed that between 5 and 10 percent of diamonds produced annually in a particular region are lost due to theft or pilferage. The destination of the uncut diamonds lost to this "leakage" is the illicit diamond market. Moreover, due to the breakdown of central controls in some diamond producing areas of western Africa, the profits for diamonds sold from that region have been known to help further ongoing armed conflicts by providing income to purchase arms. Consequently, these diamonds have been labelled "conflict" or "blood" diamonds.

50. Several FATF members indicated this year that they had concrete cases of criminal use of the diamond trade for money laundering. As with gold, the simplest typology involving diamonds consists of direct purchase of the diamonds with criminal proceeds. According to other reports, both natural and legal persons active in the diamond sector have been involved in more complex diamond related money laundering cases. Some of the detected schemes served as a cover for the laundering of the proceeds of illicit diamond trafficking, or else the diamond trading activity was used as a smokescreen for the laundering of proceeds generated by other criminal activity, especially illegal narcotics trafficking and various types of fraud. The more common types of laundering activity related to this sector include retail foreign exchange transactions, purchasing of gaming chips at casinos, forged or fraudulent invoicing, commingling of legitimate and illicit proceeds in the accounts of diamond trading companies, and in particular, international funds transfers among these accounts.

Example 19: Criminal attempts to launder fraud proceeds through the diamond market

A known criminal who had benefited financially from a fraud that took place outside Country A attempted to send money to jewellers. This was with a view to purchasing precious stones. The financial institution holding the account had been concerned about the individual for some time and had made several suspicious transaction reports to the FIU in Country A. The client attempted to send USD 8.2 million to the jewellers. Before this took place the bank took the commercial decision to freeze the accounts. The law enforcement agency made initial investigations and was satisfied that the attempt to buy precious stones had been an attempt to launder the proceeds of the fraud.

Example 20: Diamond trading used as a cover for laundering of illicit funds

One of the files developed by the FIU of Country Y relates to a company with its registered office in an offshore centre, whose corporate object was especially broad and which, in particular, encompassed diamond trading. The account that this company held in Country Y formed the object of numerous international funds transfers in foreign currencies originating in a tax haven. The funds, in very large sums, were then systematically and immediately withdrawn in cash. These withdrawals were made in large denominations of foreign currencies by a third party, who was a director of companies active in diamond trading. In view of the regularity of some of these operations, it was difficult to associate them with any legal commercial activity in the diamond sector, where one would expect the level of the funds generated to fluctuate. From information gathered by the FIU, it appeared that this account was used as a channelling account with the aim of hampering any investigations into the origin and ultimate destination of the funds. This file was passed on for the laundering of funds associated with illicit diamond trafficking and forms the subject of a judicial investigation by the public prosecutor's office.

51. As indicated in the introduction to this chapter, concerns have been raised – especially by the international press – about the possibility that terrorist groups may be using diamonds or access to the trade in conflict diamonds as a means of financing their activities. FATF delegations were therefore asked as part of this year's exercise to find cases or at least indicators of any connections between diamond trading and terrorist financing. Several delegations reported having found some indicators of a terrorist financing link with illicit trafficking in diamonds. One delegation provided information on

an alleged attempt to purchase 2 kg of precious stones with funds originating from the Al-Qaida terrorist group and through a former minister of the Taliban regime in Afghanistan. Two others provided actual case examples showing these links (included below).

Example 21: Laundering through diamond sector funds terrorist group

The FIU of Country F received several disclosures form different banks concerning two persons as well as one company active in the diamond trade. The persons were account holders at these banks. In the space of a few months the accounts of these different clients underwent a great number of fund transfers from and to foreign countries. Moreover a little while after the opening of his account one of the clients collected several bank cheques in dollars for significant amounts.

According to the financial information obtained by the FIU, it appeared that one of the accounts of the company was credited by significant amounts of dollars originating from companies active in the diamond industry and debited by several transfers to the Middle East in favour of a European citizen born in Africa and residing in the Middle East.

One of the directors of the company, a citizen of Country F residing in Africa, held an account at a bank also in Country F to which several transfers took place to and from foreign countries (Europe, Africa, North America, the Middle East). The transfers from foreign countries mainly took place in dollars and were then converted to the local currency to process transfers to foreign countries on the one hand and to accounts in Country F belonging to the client and his wife on the other hand. According to the police information collected by the Unit, it appeared that the prosecutor had opened a file related to trafficking in diamonds originating from Africa.

The important transfers of funds by the company trading in diamonds were mainly destined to the same person residing in the Middle East. Police sources revealed that this person as well as the client who had cashed the cheques was suspected of having bought diamonds from the rebel army of an African country and of having smuggled them into Country F on behalf of a terrorist organisation. Moreover, it appeared that certain persons and companies linked with the aforementioned clients have already been transmitted by the FIU in other files for money laundering derived from organised crime.

Example 22: Diamond trading allegedly finances terrorist organisation

This case consists of two parts. Its common denominator is traffic in precious stones. The starting point was a transaction in diamonds to finance an Islamic terrorist organisation. A diamond dealer from a Middle Eastern country but established in a Europe seems to have been used as an intermediary to sell diamonds bought at market prices in a west African country and shipped through a neighbouring African country. The profits on this transaction were apparently used to fund Osama Ben Laden's Al Qaïda organisation.

The person concerned is on a list of 135 persons forbidden to travel under UN Security Council Resolution 1343 (2001) because of his involvement in diamond trafficking in favour of a revolutionary movement in Sierra Leone. Some years ago, he reportedly participated in a series of terrorist attacks in Africa.

Moreover, this individual and his family seem to have relations with another family of diamond dealers – with the same origins – whose bank account movements may conceal a particularly interesting money laundering mechanism.

The parties involved in this second part took a loan of about USD 3.8 million with a bank in Country T. It was not so much the use of these funds which raised a problem (as their origin was not under a cloud) as the debt repayment terms, which could allow the borrowers to repay their loan by laundering the proceeds from crime,

probably diamond trafficking. Moreover, before the funds were transferred for payment in Country T, they had probably already been pre-laundered through intermediate banks in different European countries.

52. The cases involving alleged terrorist links seem to follow the same typologies as those carried out for the purpose of non-terrorist money laundering. Indeed, often the only difference between these and the other cases is that one of the individuals involved in the scheme has been included on one of the lists published by the United Nations Security Council.[14] It can be assumed therefore that terrorist groups may be exploiting the same channels for moving funds or obscuring the links to their activities as those used by non-terrorist groups. Given the relatively small number of concrete cases in which a connection can be conclusively demonstrated, it is impossible to determine the degree that terrorist groups could be using the diamond trade.

53. The gold trade and the diamond industry are two sectors that appear to show considerable vulnerability to being exploited for money laundering and – to an unknown extent – for terrorist financing as well. The factors described above, that is, the high intrinsic worth and their compact nature, appear to make the gold and diamond sectors attractive as a cover for laundering illegal funds from other crimes as well as a laundering vehicle in and of itself. The FATF experts provided some material on current measures or controls that are intended to assist in detecting money laundering through trade in high-value items. Despite the existence of these measures in many jurisdictions, it does not appear that they are enforced consistently across the entire FATF membership. Indeed, at least one delegation admitted that the diamond and gold trade were not well known or understood in his jurisdiction and called for additional attention to be paid to this area. A few European jurisdictions indicated that the new European Directive on money laundering[15] will finally provide a common framework for including trade in gold, diamonds and other high value items within anti-money laundering monitoring systems.

[14] UN Security Council Resolutions 1267 (1999) and 1390 (2002)

[15] Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering. This Directive must be implemented by 15 June 2003.

CHAPTER 4: OTHER TERRORIST FINANCING & MONEY LAUNDERING TRENDS

54. For this year's typologies exercise, the FATF experts were also asked to provide information on other trends in the area of terrorist financing or money laundering that they may have identified during the past year. As part of this effort, they were invited to provide statistical data relating to disclosures of suspicious financial transactions and any relevant analyses. This chapter groups together a selection of this material along with a few more case examples provided in the written contributions of FATF delegations.

Statistics

55. In the weeks immediately following the September 11th terrorist attacks, a significant increase in suspicious transaction reporting occurred in many jurisdictions. This sudden change in reporting patterns was already indicated during last year's typologies exercise. Similarly, the introduction of the euro in physical form at the beginning of 2002[16] was touched on in the FATF-XIII exercise; however, incomplete information was available at that time. FATF members were therefore asked to follow up on this change in reporting patterns after September 11th and through 2002 for this year's exercise.

56. Statistics on suspicious transaction reporting submitted by FATF members showed a general upward trend in most members even before the September 11th terrorist attacks. For those members contributing material on this issue, the increases in reporting after the attacks ranged from around a quarter to more than double the rate for the prior year. The higher rate of reporting also appears to have continued in many jurisdictions rather than peaking and tapering off as might have been expected. Some analyses attributed the first wave of reporting in the last part of 2001 and early 2002 as a direct reaction to the attacks, that is, increased awareness of the threat of terrorist misuse of the financial system rather than a sudden increase in such activity. Where the reporting rate has remained high in the subsequent period, at least one member indicated finding primarily reports related to persons and entities included on international lists[17] of terrorists or terrorist related entities.

57. With regard to introduction of the euro, reported increases in the overall number of disclosures appear for the most part to be hidden by the increase in terrorist financing reporting. There seems to have been no appreciable effect of the introduction of the euro on suspicious transaction reporting in non-Euro zone members. For those Euro zone members that offered some analysis on this subject, the effect of the euro introduction was reflected to varying degrees in suspicious transaction reporting – from no effect to considerable. The effect was felt primarily in certain parts of the financial sector, particularly for bureaux de change. One jurisdiction reported that over 80 percent of suspicious transactions during the euro introduction were made by bureaux de change. A number of FATF members had not yet completely analysed their data on suspicious transactions reporting for 2002; therefore, it is difficult to draw meaningful conclusions on this issue at present.

Financial Profile of the Terrorists Involved in the September 11th Attacks

58. US authorities have been able to put together a profile of the individual hijackers and their financial activity in the period prior to the September 11th terrorist attacks. This information was developed from material from a variety of sources, and it details how the hijackers received and

[16] FATF members which are also part of the Euro zone include Austria, Belgium, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal and Spain.

[17] UN Security Council Resolutions 1267 (1999) and 1390 (2002); US Executive Order 13224, 23 September 2001 (with updates); EU Council Decision (EC) Nº 927/2001 of 27 December 2001, EU Council Common Position of 27 December 2001, EU Council Regulation Nº 881/2002 of 27 May 2002

managed their funding, as well as how they paid for their flight training and other expenses. The US analysis confirms the earlier observations that transactions performed by the persons involved were relatively low and that, for the most part, the conventional financial system was used for setting up accounts, moving funds and paying for expenses[18].

Insurance and Money Laundering

59. A few FATF experts submitted case examples that show the vulnerabilities of the insurance sector to misuse for money laundering. The primary emphasis in the examples is on the investment aspect of life insurance or life insurance policies. With regard to this investment side of insurance, a number of aspects of the sector seem to indicate that the vulnerabilities to money laundering are similar to those for the securities sector (as discussed in Chapter 2). For example, in some jurisdictions, life insurance policies are viewed as another sort of investment vehicle similar to investment in the securities market. Another similarity between the sectors, according to one FATF expert, is that the insurance broker may often be the weak link in implementing anti-money laundering measures. In the insurance case described by this expert, more details on this and other weaknesses were provided:

- Insurance brokers had no or little training in anti-money laundering issues and were utilised to place cash funds into various financial institutions. The focus of the brokers was on selling the insurance products, and thus they often overlooked signs of money laundering, such as pre-signed forms, lack of explanation for wealth or unusual methods for paying insurance premiums.

- Even with a sales-driven objective, the insurance brokers had a great deal of control and freedom regarding policies. Brokers often maintained pre-signed payment instructions for policy withdrawals to enable clients to effect such withdrawals with a telephone call. Brokers sometimes paid insurance premiums from their own accounts; presumably they were subsequently reimbursed by the client in cash.

- Some insurance companies failed to identify indicators of money laundering, such as payments for insurance products by unrelated third parties or through use of consecutively number cheques or money orders.

- Certain insurance policies operated in the same manner as unit trusts or mutual funds. The customer could then over-fund the policy, moving funds into and out of the policy for the cost of early withdrawal penalties. When such funds are reimbursed by the insurance company (by cheque, for example), the potential launderer has successfully obscured the link between the funds and the original criminal activity that generated them.

- In addition to a lack of knowledge of the client and the source of his or her funds, insurance companies often had little knowledge of the complex pyramid of sub-brokers employed by their agents.

[18] US Treasury Financial Crimes Enforcement Network (FinCEN) *Suspicious Activity Report Review* (Issue Nº 4, August 2002), available from: http://www.fincen.gov; and FBI testimony to US Congress available from http://www.fbi.gov/congress/congress02/lormel021202.htm.

Example 23: Criminal funds laundered through payment of insurance premiums

A company director from Company W, Mr. H, set up a money laundering scheme involving two companies, each one established under two different legal systems. Both of the entities were to provide financial services and providing financial guarantees for which he would act as director.

These companies wired the sum of USD 1.1 million to the accounts of Mr. H in Country S. It is likely that the funds originated in some sort of criminal activity and had already been introduced in some way into the financial system. Mr. H also received transfers from Country C.

Funds were transferred from one account to another (several types of accounts were involved, including both current and savings accounts). Through one of these transfers, the funds were transferred to Country U from a current account in order to make payments on life insurance policies. The investment in these policies was the main mechanism in the scheme for laundering the funds. The premiums paid for the life insurance policies in Country U amounted to some USD 1.2 million and represented the last step in the laundering operation.

Example 24: Drug trafficker launders funds through purchase of life insurance policy

A person (later arrested for drug trafficking) made a financial investment (life insurance) of USD 250,000 by means of an insurance broker. He acted as follows: He contacted an insurance broker and delivered a total amount of USD 250,000 in three cash instalments. The insurance broker did not report the delivery of that amount and deposited the three instalments in the bank. These actions raise no suspicion at the bank, since the insurance broker is known to them as being connected to the insurance branch. The insurance broker delivers, afterwards, to the insurance company responsible for making the financial investment, three cheques from a bank account under his name, totalling USD 250,000, thus avoiding the raising suspicions with the insurance company.

60. Given the apparent similarities between the insurance and securities sectors in so far as how they both may be vulnerable to money laundering, it may be useful to examine the insurance sector in more depth in a future typologies exercise.

Credit and Debit Cards and Money Laundering

61. One FATF member submitted material on a study conducted to determine how credit and debit cards could be used for money laundering. The study was based on examination of relevant disclosures of suspicious transactions, and it identified a number of patterns of suspicious activity associated with such cards. Structured cash payments for outstanding credit card balances were the most common activity detected, often with relatively large sums as payments. In a few instances, third parties attempted to make cash payments on behalf of the card holder. A large number of identified scenarios involved some sort of credit card fraud, that is, where lost or stolen cards are used by a third party. Yet another pattern of activity was using cash advances from credit card accounts to purchase cashier's cheques or to wire funds to foreign destinations. There were also some instances of depositing cash advances into savings or current accounts.

62. The findings described by the FATF member in this area may be indicative of more widespread activity that could relate to various financial crimes, as well as money laundering and terrorist financing. It would also therefore be useful if this subject could be examined as part of a future FATF typologies exercise.

CONCLUSION

63. Terrorist misuse of the financial system remains a key focus in the FATF's work in examining typologies. For this reason, the FATF-XIV typologies exercise has devoted a significant effort on better understanding the phenomenon. This year, the exercise followed up on earlier indications that non-profit organisations were somehow being misused for terrorist financing. Information provided by FATF delegations and experts participating in this year's exercise confirm that the NPO sector is vulnerable to abuse, and several examples were given that appear to confirm this observation. The experts believe that NPOs, given the diversity of form and oversight systems, can be used by terrorist groups either as a means of collecting funds for eventual support of terrorist activity or as a cover for the movement of such funds. In many cases, the NPOs themselves are not entirely aware of this misuse.

64. The FATF typologies exercise also looked at informal money or value transfer (IMVT) systems again to see whether they could be used for moving terrorist funds. These complex systems exist alongside or, in some jurisdictions, in place of conventional financial services for moving funds, and they thus are often also referred to as *alternative remittance* or *underground banking*, as well as by certain regionally specific terms such as *hawala*, *hundi*, *fei-chien* or *black market peso exchange*. The primary purpose for such systems is to move legitimately earned funds from one geographic area to another, and certain of them predate Western or conventional banking systems by several centuries. Nevertheless, they generally operate outside traditional financial regulatory structures and thus are vulnerable to being used by terrorists as well as other criminals that desire to move funds. Some FATF members provided a few examples of what appears to be the use of IMVT systems by terrorists or organisations that may be assisting them. A few experts also provided examples in which some groups were attempting to get around requirements to register IMVT services by re-establishing themselves as non-profit organisations.

65. Typologies work this year examined other areas in which the primary risks or vulnerabilities lie in their potential use for money laundering. The securities sector, for example, has long been viewed by certain FATF experts as a mechanism for the layering of illegal funds. Case examples provided for the exercise indicated that in some instances it is also still possible to introduce cash proceeds into the financial system through certain securities markets by co-opting professional operators in the sector. Some experts also indicated that a presumption within some countries' securities sector that all know your customer and due diligence procedures have been performed for customers or funds coming from elsewhere in the financial system leads to another potential weakness that can be exploited by those desiring to launder money through the securities market. In a few examples, FATF experts showed still another advantage for launderers who decide to use the securities market for their activities. Besides successfully laundering their funds, some schemes using market mechanisms have the potential to produce profit from the laundering scheme.

66. The markets for gold, diamonds, and other precious metals or gemstones have often been cited as potential areas through which illegal funds may be channelled. The inherent high-value of the substances, their ability to retain their value despite the form, and ease of convertibility, along with their compact and relatively easily transportable nature also make them attractive to the money launderer. Gold and diamonds, in particular, can be used both as a source of illegal value to be laundered – through smuggling or illegal trade – or as the actual laundering vehicle – through the outright buying and selling. The primary sources of illegal funds laundered through such markets are illegal narcotics trafficking, organised crime activities and smuggling (including in the substances themselves). FATF experts were also able to provide a few examples in which gold or diamond trading has been used to move funds or simply to store value for persons or groups associated with terrorism.

67. Finally, in the area of other trends for money laundering and terrorist financing, FATF experts provided additional material both in their written contributions for the exercise and during the experts meeting itself. With regard to statistics on disclosures of suspicious transactions, the experts noted that the September 11th terrorist attacks have precipitated a marked increase in reporting that has, for many jurisdictions, not yet abated. The introduction of the euro in physical form appears only to have resulted in increased reporting in certain financial sectors just prior to and after the introduction and only in certain Euro zone members. A few case examples were provided this year that deal with insurance as a means of laundering criminal funds. From these examples, it appears that the insurance sector may possess similar potential laundering vulnerabilities to those of the securities sector. This last area may warrant further study in the context of future FATF typologies exercises.