SECRETARIA DE HACIENDA Y CREDITO PUBLICO

COMISION NACIONAL DE SEGUROS Y FIANZAS

FIANZA
RECIBIDO
MAYO 8 2002
MEXICO, D.F.

México, D. F., 2 de mayo de 2002

OFICIO-CIRCULAR SF-21/02

ASUNTO: Se da a conocer Reporte del Ejercicio de Tipologías 2000-2001 del Grupo de Acción Financiera sobre el Blanqueo de Capitales (GAFI).

A LAS INSTITUCIONES Y SOCIEDADES MUTUALISTAS DE SEGUROS E INSTITUCIONES DE FIANZAS

La Secretaría de Hacienda y Crédito Público, Dirección General de Seguros y Valores, mediante Oficio 366-III-A-1460 de 18 de abril del presente año, solicita hacer del conocimiento de esas instituciones y sociedades, el Reporte del Ejercicio de Tipologías 2000-2001, aprobado por el Pleno del Grupo de Acción Financiera sobre el Blanqueo de Capitales (GAFI) a finales del mes de enero último, en su reunión celebrada en Hong Kong, China.

Cabe señalar que dicho Reporte, incluye una sección especializada sobre el financiamiento al terrorismo, acorde con la expansión de misión del citado Grupo, decidida a partir de los actos terroristas perpetrados el 11 de septiembre pasado en contra de los Estados Unidos de América, además de examinarse asuntos relacionados con banca corresponsal y privada, personas "políticamente expuestas", acciones al portador y otros instrumentos negociables, coordinación entre grupos de delincuencia organizada y la introducción del Euro. Asimismo, se inicia un estudio sobre la relación entre los reportes de operaciones y los casos de lavado detectados por las autoridades competentes.

Por lo expuesto, se anexa al presente copia del Reporte del Ejercicio de Tipologías 2000-2001, aprobado por el Pleno del Grupo de Acción Financiera sobre el Blanqueo de Capitales (GAFI).

Lo anterior se hace de su conocimiento con fundamento en los artículos 108 fracción IV de la Ley General de Instituciones y Sociedades Mutualistas de Seguros, 68 fracción VI de la Ley Federal de Instituciones de Fianzas y de conformidad con el Acuerdo por el que la Junta de Gobierno de la Comisión Nacional de Seguros y Fianzas delega en el presidente la facultad de emitir las disposiciones necesarias para el ejercicio de las facultades que la ley le otorga a dicha Comisión, y para el eficaz cumplimiento de la misma y de las reglas y reglamentos, emitido el 2 de diciembre de 1998 y publicado en el Diario Oficial de la Federación el 4 de enero de 1999.

Atentamente
SUFRAGIO EFECTIVO. NO REELECCION.
COMISION NACIONAL DE SEGUROS Y FIANZAS
El Presidente

LIC. MANUEL S. AGUILERA VERDUZCO

ANEXO

GODF-1

Financial Action Task Force
on Money Laundering

Groupe d'action financière
sur le blanchiment de capitaux

Report on Money Laundering Typologies 2001-2002

FATF-XIII

1 February 2002

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

Contact@fatf-gafi.org

TY2002_en
01.02.2002/12h00

TABLE OF CONTENTS

LIST OF CASE EXAMPLES

INTRODUCTION

1. Combating money laundering has been a core element of the international fight against serious crime for over twelve years. The underlying goal of this effort to disrupt the financial support for criminals and denying them access to legitimate financial systems. Money laundering is an evolving activity, however, and must be continuously monitored in all its various forms in order for measures taken in this effort to be timely and effective. The Financial Action Task Force (FATF) examines the methods and trends of money laundering through its annual typologies exercise and uses this work, in part, to ensure that the Forty Recommendations are up to date.

2. The FATF held this year's meeting of experts on money laundering typologies on 19 and 20 November 2001. The meeting took place in Wellington, New Zealand under the chairmanship of Detective Superintendent Bill Bishop, Police National Crime Manager, New Zealand, and included representatives from the following FATF members: Australia; Austria; Belgium; Canada; Denmark; Finland; France; Hong Kong, China; Ireland; Italy; Japan; Luxembourg; Mexico; the Netherlands; New Zealand; Norway; Portugal; Singapore; Spain; Sweden; Switzerland; Turkey; the United Kingdom; and the United States. The Asia Pacific Group on Money Laundering (Cook Islands) was present at the meeting along with the following observer international organisations: the Egmont Group of financial intelligence units, the International Monetary Fund (IMF), Interpol, the World Bank and the World Customs Organisation (WCO).

3. In early September 2001, the FATF agreed on a series of topics for the FATF-XIII typologies exercise. Following the September 11th terrorist attacks in the United States, the FATF revised its remit to include terrorist financing and modified the programme for the typologies exercise to include this topic. Besides this additional specialised topic then, this year's exercise examined money laundering issues as related to correspondent banking, private banking and "politically exposed persons", bearer shares and other negotiable instruments, co-ordination among organised crime groups and the introduction of euro in banknote and coin form. As a final theme for the exercise, FATF members also began a first comprehensive study of the relationship between suspicious transaction reports (STRs) and money laundering cases.

4. This document is the report on the FATF-XIII typologies exercise. FATF delegations and invited experts submitted written material to serve as the starting point for discussions on each of the topics and to provide additional explanatory or illustrative information for the report. It therefore brings together the issues as discussed at the Wellington meeting as well as incorporating the supplementary material based on the written submissions of participating FATF members or observer organisations. The report is divided into chapters on each of the specialised topics mentioned in the preceding paragraph and includes another chapter on STRs and money laundering cases. Because of the addition of terrorist financing to this year's typologies programme and the limitations of a two-day meeting, two topics – co-ordination among organised crime groups and introduction of euro banknotes – could not be discussed in Wellington. The chapters on these two subjects consist, therefore, of summaries of the written information furnished by participants in the exercise.

5. Case examples taken from the written contributions of FATF members have been included throughout the report. In most instances, the texts of the examples are given as provided by the contributing jurisdictions to offer some more insight into issues confronting anti-money laundering authorities. Country names, currencies and certain other details have been modified in an effort to protect sensitive details of specific investigations or reports.

CHAPTER 1 - TERRORIST FINANCING

6. During last year's typologies exercise, FATF experts focused for the first time on how terrorists conceal or move funds in support of their operations. The objectives of this work were to identify the financing methods used by terrorists and how they differ from those used by other criminal groups. The exercise also sought to determine whether distinctions between legal and illegal funding sources affect the ability of countries to use anti-money laundering measures in detecting, investigating and prosecuting terrorist related financial activity.

7. At the 2000-2001 typologies exercise, the FATF experts found that there was in fact little difference between terrorist and other criminal methods in the use of the financial system. For a few jurisdictions, the fact that terrorist groups may rely on legal sources of revenue mattered little in their ability to target terrorist financial networks. For others, however, the fact that terrorist financing might not meet the definition of money laundering meant that they were limited in the actions they could take against terrorist monies in the framework of anti-money laundering laws. All the experts agreed that terrorism was a serious crime.

8. In the aftermath of the September 11 terrorist attacks in the United States and the discovery of the wide geographic extent of the terrorist financial infrastructure that enabled them, governments moved quickly to create new counter-measures that could be specifically used to detect and dismantle such structures. Building on the existing expertise of the FATF, its members expanded the remit of the Task Force to include terrorist financing and issued a set of Special Recommendations to address the issue. The FATF also refocused this year's typologies exercise by calling on the experts to examine terrorist financing again with the aim of developing guidance for financial institutions. This guidance could be used to help detect transactions potentially related to terrorists and terrorist groups, as well as the persons and entities that support them.

Characteristics of terrorist financing

9. According to one definition of terrorism, it has as its primary objective "to intimidate a population, or to compel a Government of an international organisation to do or abstain from doing any act".[1] In contrast, criminal organisations are supposedly only motivated by financial gain. While this difference may be true to some extent, terrorist organisations require financial support in order to achieve their aims. A successful terrorist group is therefore, as with a criminal organisation, one that is able to build and maintain an effective financial infrastructure. For this it must develop sources of funding, a means of laundering those funds and then finally a way to ensure that the funds can be used to obtain material and other logistical items needed to commit terrorist acts.

Terrorist fundraising

10. In discussing the financing of terrorism it is necessary to start with a discussion of the sources of income. According to some experts, there are two primary sources of financing for terrorist activities. The first method involves obtaining financial support from States or structures with large enough organisations to be able to collect and then make the funds available to the terrorist organisation. It is believed that this so-called State-sponsored terrorism has declined in recent years and has been superseded by backing from other sources. An individual with sufficient financial means may also provide substantial funding to terrorist groups, for example, as is believed to have been the case with the September 11th terrorist attacks. Osama bin Laden, considered the mastermind behind these attacks, is thought to have contributed significant amounts of his personal fortune to the establishment and support of the Al-Qaeda terrorist network, along with the Taliban regime that formerly ruled Afghanistan.

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

11. The second method for raising funds for the terrorist organisations is to obtain them directly from various "revenue-generating" activities. These activities may include criminal acts; in this way they may appear similar to ordinary criminal organisations. Unlike such organisations however, terrorist groups may also derive a portion of their revenues from legitimately earned income. How much of a role legal monies play in the support of terrorism seems to vary according to the terrorist group and whether its source of funds is in the same geographic location as its terrorist acts. One FATF expert, in describing a terrorist group active in his country, stated that its principal source of funds was through kidnapping and extortion. In this scenario, ransoms paid to retrieve hostages, along with the "revolutionary tax" or protection money demanded of businesses, provide needed financial resources but also play a secondary role as one other means of intimidating the target population. Besides kidnapping and extortion, terrorist groups may engage in large-scale smuggling operations, various types of fraud, thefts and robbery, and narcotics trafficking.

Example 1: Credit card fraud supports terrorist network

One operation discovered that a single individual fraudulently obtained at least twenty-one Visa and MasterCards using two different versions of his name. Seven of those cards came from the same banking group. Debts attributed to those cards totalled just over USD 85,000. Also involved in this scheme were other manipulations of credit cards, including the skimming of funds from innocent cardholders. This method entails copying the details from the magnetic strip of legitimate cards onto duplicate cards, which are used to make purchases or cash withdrawals until the real cardholder discovers the fraud. The production of fraudulent credit cards has been assisted by the availability of programmes through the internet.

Example 2: Terrorists acquire funds through criminal activity

In late 1999, a network of religious extremists was broken up in an FATF member jurisdiction (Country A) as its members were preparing violent acts on its soil for the end-of-year festivities. The inquiry launched by law enforcement authorities revealed the existence of links between this network and a number of individuals living in another FATF country (Country B) and known to the specialised services for their religious extremism.

Investigations were undertaken in Country B as part of the judicial inquiry initiated on the basis of the information provided by the authorities of Country A. The investigation established that this group of ten individuals, most of whom had fought in a European regional conflict, was implicated in a number of armed attacks against several shops in early 1996 and in an attack on an armoured truck in a shopping centre car park of the same year, during which automatic weapons, rocket launchers and grenades had been used.

This group's violent acts in fact formed just one element in an entire logistical set-up working for a much larger Islamic terrorist organisation whose ramifications extended beyond Country A to three more FATF countries. The ordinary criminal offences were designed to obtain funds to serve "the cause", whilst another group dealt with trafficking false administrative documents, collecting information and clandestine movement of personnel. The members of the network were recently convicted of, among others, armed robbery and criminal association.

Legal sources of terrorist financing

12. The ideological rationale for some terrorist movements means that individual terrorists or terrorist groups may sometimes rely on legally generated sources of income. As mentioned above, this is a key difference between terrorist groups and traditional criminal organisations. One FATF member reported, for example, that the supporters of a national liberation movement from a south Asian country were carrying out ostensibly legal activities in that FATF country to obtain financial resources. They raise these funds by infiltrating and taking control of institutions within the immigrant community located there. Some of the specific fundraising methods mentioned by the expert include:

- Collection of membership dues and / or subscriptions;
- Sale of publications;
- Speaking tours, cultural and social events;
- Door-to-door solicitation within the community;
- Appeals to wealthy members of the community; and

- Donations of a portion of their personal earnings.

13. The most effective means of raising funds, according to this member, is through community solicitation and fundraising appeals, often in the name of organisations with the status of a charitable or relief organisation. The members of the community are led to believe that they are giving for a good cause, and in many cases the charities to which donations are given are in fact legitimate in the sense that the charities do carry out some of the work they purport to do. Most of the members of the organisation, however, have no knowledge that a portion of the funds raised by the charity is being diverted to terrorist causes.

14. In another example, an organisation raised funds from membership fees and by income from various businesses dealing in, among other things, computers, publishing, construction, and food production. This same group also required that certain of its members donate all of their properties, as well as a portion of their personal income.

Example 3: Terrorists collect funds from lawful sources

In 1996, a number of individuals known to belong to the religious extremist groups established in the south-east of an FATF country (Country C) convinced wealthy foreign nationals, living for unspecified reasons in Country C, to finance the construction of a place of worship. These wealthy individuals were suspected of assisting in the concealment of part of the activities of a terrorist group. It was later established that "S", a businessman in the building sector, had bought the building intended to house the place of worship and had renovated it using funds from one of his companies. He then transferred the ownership of this building, for a large profit, to Group Y belonging to the wealthy foreigners mentioned above.

This place of prayer intended for the local community in fact also served as a place to lodge clandestine "travellers" from extremist circles and collect funds. For example, soon after the work was completed, it was noticed that the place of worship was receiving large donations (millions of dollars) from other wealthy foreign businessmen. Moreover, a Group Y worker was said to have convinced his employers that a "foundation" would be more suitable for collecting and using large funds without attracting the attention of local authorities. A foundation was thus reportedly established for this purpose.

It is also believed that part of "S's" activities in heading a multipurpose international financial network (for which investments allegedly stood at USD 53 million for Country C in 1999 alone) was to provide support to a terrorist network. "S" had made a number of trips to Afghanistan and the United States. Amongst his assets were several companies registered in Country C and elsewhere. One of these companies, located in the capital of Country C, was allegedly a platform for collecting funds. "S" also purchased several buildings in the south of Country C with the potential collusion of a notary and a financial institution.

When the authorities of Country C blocked a property transaction on the basis of the foreign investment regulations, the financial institution's director stepped in to support his client's transaction and the notary presented a purchase document for the building thus ensuring that the relevant authorisation was delivered. The funds held by the bank were then transferred to another account in a bank in an NCCT jurisdiction[2] to conceal their origin when they were used in Country C.

Even though a formal link has not as yet been established between the more or less legal activities of the parties in Country C and abroad and the financing of terrorist activities carried out under the authority a specific terrorist network, the investigators suspect that at least part of the proceeds from these activities have been used for this purpose.

Laundering of terrorist related funds

15. From a technical perspective, the methods used by terrorists and their associates to generate funds from illegal sources differ little from those used by traditional criminal organisations. Logically then, terrorist groups must also find ways to launder these illicit funds in order to be able to use the funds without drawing the attention of authorities. In last year's examination of terrorist related financial activity, the FATF experts concluded that terrorists and their support organisations use the same laundering methods as criminal groups, and the cases discussed this year appear to provide further evidence of this observation. Some of the particular methods mentioned by experts this year

[2] Countries identified through the FATF initiative to identify non-cooperative countries or territories (NCCTs) in the fight against money laundering. For more information, see the FATF website: http://www.fatf-gafi.org.

in connection with various terrorist groups include: cash smuggling (both by couriers or bulk cash shipments), structured deposits to or withdrawals from bank accounts, purchases of various types of monetary instruments (travellers' cheques, bank cheques, money orders), use of credit or debit cards, and wire transfers. There have also been indications that some forms of underground banking (particularly the hawala system[3]) have had a role in moving terrorist related funds.

Example 4: Suspicious money transfers and relief organisation

Suspicious transaction reports (STRs) were filed by financial institutions on transactions totalling USD 9 million involving structured cash deposits and deposits of business, payroll and social benefit cheques. Deposited funds were subsequently transferred within one or two days to a company located abroad. The deposit and wire transfer activity involved 37 individuals, four businesses and 44 accounts. Two of the businesses appear to be ethnic based money remittance companies; one is described as a relief organisation at the same location as one of the money remittance businesses; the fourth business, was the beneficiary of the money transfer activity. The majority of the wire transfers were sent to two accounts in the foreign location.

Example 5: Purchase of cheques and wire transfers by alleged terrorists

Suspicious transaction reports outlined unusual activity involving three grocery markets, two of which share a common location. The activity was conducted by individuals of the same ethnic origin using a single address, which corresponds to one of the business locations. Two individuals employed by a grocery store and a third whose occupation was unknown each deposited funds just under applicable reporting thresholds and immediately drew cheques payable to a fourth individual. The cheques cleared through two different banks in a foreign country. All three bank customers supplied the same address. In addition, two individuals associated with a second grocery store located at the common address above each purchased bank cheques just under the applicable reporting threshold at the same bank branch, at the same time but from different tellers. One of the cheques was purchased on behalf of the second grocery store, the other on behalf of third party. The cheques were payable to two different individuals, one of whom shared the same last name as one of the purchasers. In related activity, a third business used the common address discussed above when opening a business account which immediately received a USD 20,000 wire transfer from a wholesale grocery located in another region of the country. Filings of cash transaction reports indicate that a total of about USD 72,000 was withdrawn in cash from other accounts associated with this business.

Example 6: Suspect money order purchases at money remittance company

In Country D, both a money remittance company and a financial institution filed suspicious transaction reports outlining the movement of approximately USD 7 million in money orders through the account of a foreign business. The wire remittance company reported various individuals purchasing money orders at the maximum face value of USD 500 - 1,000 and in sequential order. Purchases were made at multiple locations, primarily in the north-east part of Country D, with several instances also reported in the south-east. The money orders were made payable to various individuals, negotiated through banks in an NCCT jurisdiction and later cleared through three Country D financial institutions. The foreign business endorsed the money orders. In some instances, the funds were then credited to accounts at other Country D banks or foreign financial institutions (one in an NCCT country, the second location not identified). Suspicious transaction reports filed by the institution indicated similar purchases of money orders in the north-east of the country and negotiated at the foreign business. Various beneficiaries were identified, and the amounts ranged from USD 5,000 to USD 11,000. The foreign business identified by the money remittance company was also identified as a secondary beneficiary. The money orders cleared through a foreign bank's correspondent account at the Country D financial institution.

Further observations on terrorist financing

16. As was observed during last year's typologies exercise, the difference between legally and illegally obtained proceeds raises an important legal problem as far as applying anti-money laundering measures to terrorist financing. Money laundering has generally been defined as a process whereby funds obtained or generated by criminal activity are moved or concealed. The terrorist's ultimate aim on the other hand is not to generate profit from his fundraising mechanisms but to obtain resources to support his operations. In a number of countries, terrorist financing thus may not yet be included as a

[3] For more information on the hawala system of alternate remittance / underground banking, see the 1999-2000 *FATF Report on Money Laundering Typologies*, 3 February 2001 (pp. 4-8).

predicate offence for money laundering, and it may be impossible therefore to apply preventive and repressive measures specifically targeting this terrorist activity.

17. When terrorists or terrorist organisations obtain their financial support from legal sources (donations, sales of publications, etc.), there are certain factors that make detecting and tracing these funds more difficult. For example, the apparent legal source of this funding may mean that there are few, if any, indicators that would make an individual financial transaction or series of transactions stand out as linked to terrorist activities.

18. Charities or non-profit organisations and other legal entities have been cited as possibly playing an important role in terrorist financing. Indeed, one FATF member reported several instances of involvement of charities in facilitating the financing of terrorism. The examples submitted as part of this typologies exercise this year seem to show that some non-profit organisations have served either as a direct source of income or as a cover for money laundering activities. Nevertheless, it is unlikely that the presence of such an organisation by itself could serve as a possible indicator of terrorist financial operations. This issue will require additional study as more is learned about the financing behind the September 11th events and other terrorist activity.

19. Other important aspects of terrorist financing that make its detection more difficult are the size and nature of the transactions involved. Several of the experts mentioned that the funding needed to mount a terrorist attack does not always call for large sums of money, and the associated transactions are usually not complex. For example, an examination of the financial connections between the September 11th hijackers and their overseas accounts showed that most of the individual transactions were small sums, that is, less than USD 10,000, and in most cases the operations consisted of nothing more than wire transfers. The individuals were ostensibly foreign students who appeared to be receiving money from their parents or in the form of grants for their studies, thus the transactions would not have been identified as needing additional scrutiny by the financial institutions involved.

20. Several FATF experts pointed out that it is the "active service" personnel or the terrorists who actually commit the terrorist act that may be most difficult to detect through suspicious financial transactions alone. To better identify these individuals, counter-terrorism authorities will need to rely on financial information along with other intelligence. Financial institutions themselves will also need to have specific guidance on the methods of terrorist financing and will likewise have to use this material in conjunction with other sources of information, such as the various lists of persons, entities and jurisdictions of concern in the fight against terrorism. Investigators in the United States and other countries have learned a great deal about the global financial infrastructure that supported the September 11th attacks. However, it is still too early in the investigation to have a complete picture of this infrastructure. As a first step toward assisting financial institutions in identifying factors that may identify potential terrorist financing, the FATF has nevertheless developed a series of general indicators based on the experience of its members in dealing with this problem and other available information.

Example 7: Simple transactions found to be suspect

In October 2001, the financial intelligence unit (FIU) of Country E forwarded to the judicial authorities some ten files with relation to money laundering derived from terrorism. In general, the files dealt with instances in which simple operations had been performed (retail foreign exchange operations, international transfer of funds) revealing links with other countries. Some of the customers had police records, particularly for trafficking in narcotics and weapons, and were linked with foreign terrorist groups.

One of the files submitted by the FIU in relation with terrorism is of particular interest in this respect: the customer was holder of a current account and of a savings account in the reporting financial institution. Moreover, he purchased securities and a life insurance with single premium in the same institution. He performed several transfers from his current account to beneficiaries in different countries. The suspicions of the bank arose from the fact that a name similar to the customer's appeared on the consolidated list of persons and/or entities included in the UN Security Council Committee on Afghanistan

(S/RES/1333(2000)) and Regulation 1354/2001 of the European Commission). The suspicion of the bank was strengthened by the fact that the customer had been progressively withdrawing funds he held at this bank since the end of April 2001. He successively cleared out his savings account, sold the securities he had purchased before the expiry date, repurchased his life insurance premium and finally transferred his remaining funds to the European country where he resided. The last operation he performed occurred at the end of August 2001, that is, about two weeks before the attacks in the United States. The bank has had no more contact with this customer since then.

Counter-measures

21. In looking at counter-measures against terrorist financing, mention should first be made of the work undertaken by the United Nations to address this issue. The principal efforts by the United Nations in this regard relate to promoting the ratification of the International Convention for the Suppression of the Financing of Terrorism from 9 December 1999 and to freezing or blocking of terrorist funds and assets as required by UN Security Council Resolution 1373(2001) and various others.[4] The Convention has been signed by 132 States; however, with only 16 of the 22 necessary ratifications, the Convention has not yet come into force.

22. As a consequence of the September 11th events, FATF members have taken action to establish additional measures specifically targeting terrorist financing. In October 2001, the FATF extended its remit to include terrorist financing and issued a series of eight Special Recommendations on steps that national governments should take to address such activity. FATF members agreed to implement the Special Recommendations by June 2002 and called on all other governments to do the same. In the area of prevention, the FATF proposed the establishing guidance to assist financial institutions in detecting transactions that may relate to terrorist financing and reporting them, when appropriate, under applicable suspicious or unusual transaction reporting systems. The first edition of the guidance for financial institutions is currently in development and will be published in due course.

23. Several FATF members have also begun taking action individually and through regional organisations in this area. No attempt will be made at this point to describe these national measures, as they will shortly be examined as part of the FATF process of self-assessment on terrorist financing. It should be noted as well that the United Nations has set up a Security Council Committee pursuant to S/RES 1373(2001)[5], which will also assess implementation of the requirements of that Security Council Resolution.

[4] Among these are S/RES/1363(2001), S/RES/1333(2000), S/RES/1269(1999) and S/RES/1267(1999).

[5] "Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism" ("the Counter-terrorism committee").

CHAPTER 2 - CORRESPONDENT BANKING

24. Correspondent bank accounts are accounts that financial institutions maintain with each other on their own behalf and in their own names. International correspondent banking relationships have a variety of legitimate business purposes. However, a number of FATF jurisdictions have increasingly found that these relationships are vulnerable to misuse for money laundering. Shell banks, certain offshore financial institutions and banks from non-cooperative countries and territories (NCCTs) are of particular risk to legitimate correspondent banking relationships. These concerns have been translated into several national initiatives to examine the issue[6] or give relevant guidance to their banks.

What is correspondent banking?

25. Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). By establishing multiple correspondent relationships globally, banks can undertake international financial transactions for themselves and for their customers in jurisdictions where they have no physical presence. Large international banks typically act as correspondents for thousands of other banks around the world. Respondent banks obtain a wide range of service through the correspondent relationship, including cash management (for example, interest bearing accounts in a variety of currencies), international wire transfers of funds, cheque clearing, payable-through accounts and foreign exchange services. The services offered by a correspondent bank to smaller, less well-known banks may be restricted to non-credit, cash management services. Those respondent banks judged to be sound credit risks, however, may be offered a number of credit related products (for example, letters of credit and business accounts for credit card transactions).

How can correspondent banking be misused for money laundering?

26. By their nature, correspondent banking relationships create a situation in which a credit institution carries out financial transactions on behalf of customers from another institution. This indirect relationship means that the correspondent bank provides services for individuals or entities for which it has neither verified the identities nor obtained first-hand knowledge of the respondent's customers. In correspondent banking therefore, the correspondent institution must rely on the respondent bank's having performed all of the necessary due diligence and continuous monitoring of its own customers' account activity. Some additional risks incurred by the correspondent bank include in particular:

- Assessing the quality of anti-money laundering mechanisms in place at the respondent bank. For example, a foreign respondent bank may apply less stringent anti-money laundering standards due to weaker laws and regulations, inadequate regulatory supervision, or failures in applying standards or internal controls. While the correspondent bank may be able to determine the legislation in effect for the respondent bank, it is much more difficult to know the degree and effectiveness of the supervisory regime to which the respondent is subject.

- Existence of sub-respondents through which a respondent bank may itself be offering correspondent banking facilities to other credit institutions. One FATF member stated that some banks offering correspondent facilities may not be asking their respondents about the extent to which the latter offer such facilities to other institutions. This oversight has meant in certain cases that the correspondent bank is even farther removed from knowing the identities or business activity of these sub-respondents, or even the types of financial services provided.

[6] In particular, several FATF members cited a report by the US Senate Permanent Subcommittee on Investigations as particularly influential in raising their awareness of the potential vulnerabilities of correspondent banking relationships (*Correspondent Banking: A Gateway for Money Laundering* [February 2001]).

- Monitoring individual transactions involved in large-scale transactions between correspondent accounts since the bank is usually not in contact with the originator or the beneficiary of such transactions.

27. These risks are increased by the fact that credit institutions have tended not to consider transactions performed on behalf of other institutions as high-risk activity with regard to money laundering. Many correspondent banks have simply assumed that their respondents have already performed all necessary anti-money laundering controls. Consequently, these correspondent banks believe that there is no need to carry out further due diligence measures on the clients of their respondents.

28. It is important to note, according to the observation of one expert, that the degree of due diligence exercised by some correspondent banks appears often to be determined by whether credit was being granted. Extension of credit facilities necessitates an evaluation of the foreign bank's management, finances, business activities, reputation, regulatory environment and operating procedures. However, for fee-based services – for example, wire transfers or cheque clearing – the same degree of due diligence is often not undertaken. Yet the highest risk foreign banks are rarely extended credit, so they, in effect, failed to be scrutinised in the same way as institutions seeking credit.

Example 8: Correspondent banking allegedly facilitates laundering of fraud proceeds

Subject R, citizen of an FATF member country (Country A), registered a bank (Bank X) in Country B. He then went to Bank Y in another FATF country (Country C) and set up a bank account with them in the name of Bank X, into which he transferred approximately USD 25 million in proceeds of an investment fraud perpetrated in Country C. He subsequently opened an account in the name of Bank X with a bank in a third FATF country (Country D) and transferred a substantial sum of money into this account. Finally he opened another account in the name of Bank X with a bank in Country E where over a period of four months USD 17 million of the fraudulent money was lodged. These monies were subsequently used for the purchase of high value goods.

As already stated, these funds were the proceeds of a high yield investment fraud in the Country C and funds stolen from a Country D based company by an employee. A portion of these funds made its way to Subject R's account in Country A. These funds were the subject of an STR submitted to the FIU. Although the correspondent banking procedures did not take place in Country A, the main suspect involved was a Country A citizen, and proceeds of the fraud and the laundered money were transferred to his account in Country A. Information suggests that he may have directed the transfer of the funds from this jurisdiction via on-line banking.

29. In an example provided by one FATF member, suspicious transaction reporting (STR) in one instance revealed high value suspicious wire transfer activity transiting correspondent bank accounts maintained by foreign banks at the credit institutions of that member. This activity often involved so-called "unsubstantiated entities" or shell companies. Many of these entities appeared to be incorporated or registered within the FATF member, although it was impossible to obtain reliable corporate data on them. As reflected in these STRs, shell banks[7] are also referenced in the STRs as parties to suspicious wire transfers transiting the respondent's accounts.

30. On a number of occasions, the reporting banks' preliminary background checks of the shell companies and shell banks (for example, public databases, internet, and official corporate or financial institution registration records) often failed to reveal any information on the actual operations or existence of these "unsubstantiated entities". The reporting bank's suspicions were further heightened because the respondent bank, which maintains the account of the suspected shell entity, was unable to provide any background information on the operations or existence of the particular entity. Other factors arousing suspicion regarding these accounts included numerous large volume wire transfers,

[7] *Shell banks* are institutions with no physical presence in the jurisdiction where incorporated and which are not affiliated with a regulated financial group.

frequent transactions following unusually repetitive patterns (for example, involving reappearing parties), and the fact that the direction of the wire transfer often did not appear to correspond to normal or expected business activity.

Example 9: Correspondent banking relationship facilitates transactions by shell companies

A bank in an FATF member country (Country D) monitored activity over a given month through a correspondent account maintained at the Country D bank by a bank from another FATF country (Country E). The Country D based bank detected a particular customer of the Country E bank that appears to be a shell company and has either sent wire transfers to or received wire transfers (a total of 51 received transaction totalling USD 7.4 million) from other suspected shell entities. Some of these other suspected shell companies are based in Country D and maintain accounts at a bank in Country F. The Country D reporting bank notes that some of the transactions appear to be petroleum/oil products, but sample internet searches conducted on some of these possible shell companies involved as parties to the wire transfers did not provide additional information.

The same Country D bank, in continuing to monitor the activity in the same Country E bank's correspondent account, pinpointed another suspected shell company involved in suspicious wire transfer activity. Public and official company registry searches conducted by the Country D bank did not reveal any substantiating information on the particular shell entity. Address directory searches, for example, simply led to an apartment and individual's name. Over several months, the suspected shell entity, for example, had received USD 6.4 million in wire transfers from various other suspected shell entities (some of which are also based in Country D and maintain accounts at Russian banks). At least one of these entities is the subject of prior multiple STRs submitted by this and other financial institutions.

Example 10: Correspondent banking, wire transfers facilitate transactions by shell companies

A possible shell company (Company Q) registered in an FATF member country (Country F) received several wire transfers from another vague company located offshore. The beneficiary company (Company Q) was a customer of a bank in Country G that maintained a correspondent account at the Country F bank, which submitted an STR. Company Q was reportedly involved in the transportation of oil and other raw materials (metal, timber, gas). The Country G bank, at the request of the bank in Country F, asked Company Q to provide copies of a business contract that would justify the financial activity. Rather than providing those documents to the bank, Company Q simply closed its account.

Example 11: Banks unwittingly help to launder funds through correspondent relationship

"Bank P International", in providing correspondent services to "Bank N SA", a subsidiary of "Bank N Ltd", was actually providing services to "M Bank", a shell bank licensed in Country H. In 1998, M Bank accumulated USD 17 million in deposits derived from various fraudulent activities and went on to deposit and transfer these funds through Bank N's correspondent account at Bank P.

Preventing the misuse of correspondent banking

31. Correspondent banking and the way in which correspondent relationships can be misused in the laundering of criminal proceeds is substantially a subset of customer identification issues. The FATF is examining the correspondent banking issue in the framework of its review of the FATF Forty Recommendations.[8] In the interim, FATF experts participating in this year's typologies exercise made a number of proposals for the necessary elements of any sort of best practices guidelines on the issue. These elements include:

- Establishing rigorous "know your respondent" procedures aimed at gaining a full understanding of each respondent's legitimate business. Some factors to consider include in such procedures include:

  (a) Information about the respondent bank's management, nature of the banking licence, and its major business activities;

[8] It should be noted that the Basel Committee on Banking Supervision issued guidance for financial institutions in this area as part of its publication *Customer due diligence for banks* (October 2001).

(b) Information about where the respondent is located, in particular the existence of a real physical presence within the licensing jurisdiction;
(c) Volume and nature of transactions expected to flow through the correspondent account;
(d) Identity of any third parties allowed direct access to the correspondent account (thereby using it as a "payable through" account); respondent banks should be requested to furnish and update lists of institutions to whom they offer correspondent facilities;
(e) Rigour of banking supervision in the respondent's home country; and
(f) Quality of the respondent's money laundering prevention and detection efforts.

- Exercising heightened due diligence over the correspondent relationships or, if that is not possible, close the accounts of respondent banks having weak or non-existent customer identification and know-your-customer procedures or of those that are not effectively supervised.

- Refusing to enter into, or continue, a correspondent banking relationship with a respondent in a jurisdiction where it has no physical presence (a so-called "shell bank"), which is unaffiliated with a regulated financial group, or which is established in a non-cooperative jurisdiction and is not authorised to carry out transactions with citizens of that jurisdiction. Banks should also guard against establishing relations with respondent foreign banks that permit their accounts to be used by shell banks.

- Training staff dealing with correspondent accounts to recognise higher risk circumstances or irregular activity, whether isolated transactions or trends, and submitting a suspicious or unusual transaction report where appropriate.

- Conducting periodic reviews of all of their correspondent account relationships with foreign banks to identify higher risk respondents and closing accounts with problem banks.

- Reporting to the supervisory authority and to the respective financial intelligence unit (FIU) any problems encountered with foreign respondent banks, especially when such relations cause them to end relations with the latter.

32. On this last point, some experts also indicated that perhaps a mechanism should be established that would encourage this information to be shared spontaneously with foreign counterpart FIUs and / or financial regulatory authorities. Such a mechanism would prevent a problem foreign respondent bank from going to several correspondents of the same jurisdiction in succession once turned away by one correspondent. The exchange of information between the relevant authorities would reinforce the effectiveness of such measures at the international level. National authorities could also consider creating a system to provide information on problem foreign respondent banks to their domestic financial institutions.

CHAPTER 3 - CORRUPTION AND PRIVATE BANKING

33. Examples of senior government officials involved in corruption and other types of proceeds generating crime are no longer rare occurrences. In the past few years several high visibility corruption cases involving "politically exposed persons" or PEPs and the laundering of vast amounts of criminal proceeds through various FATF jurisdictions have been detected and investigated. Some of these laundering schemes may have been facilitated by private banking operations. While the negative publicity arising from these cases has undoubtedly increased awareness of and compliance with anti-money laundering requirements within the private banking sectors of some countries, it is unclear whether an adequate level of compliance has been reached universally.

Basic concepts

34. Private banking is the term used for "preferential" banking service provided to high net worth individuals. Within the institution, this service usually entails a higher degree of discretion and confidentiality for the client in comparison with the ordinary retail customer. Financial institutions often separate private banking from other retail banking operations as part of their customer segmentation strategy, that is, specific financial services are marketed across a customer base according to the value of the service offered. Private bank accounts can be opened in the name of an individual, a commercial business, a trust, an intermediary or an investment company. These services are administered by a relationship manager and his support team who sometimes are on call 24 hours a day and 7 days a week in order to build a strong rapport and intricate knowledge of the client's financial affairs. The services offered by private bankers are often self-administered and frequently go beyond the call of duty of a normal retail banker.

35. Politically exposed persons (PEPs), according to the Basel Committee on Banking Supervision, are "individuals who are or have been entrusted with prominent public functions, including heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of publicly owned corporations and important political party officials".[9] These individuals, especially when they come from countries with a significant corruption problem, could abuse their official functions for their own financial gain through embezzlement, receipt of bribes, and other criminal activities. Often the illegal proceeds obtained by PEPs or their associates are moved overseas for the purposes of laundering, concealment and protection of value of such funds.

Effect on money laundering

36. FATF members who provided information on this topic were in agreement that private banking potentially has two main areas of vulnerability that could be exploited by corrupt PEPs or their associates. The first is when the private banker simply fails to apply appropriate and thorough due diligence to a customer and his activities. A criminal or PEP will generally seek out private banking services, as they offer the ideal opportunity for them, their family members, and close associates to carry out sophisticated and/or complex financial transactions that will further protect their illicit assets. Since a private bank is often involved in helping the client to invest or protect his or her assets, a private bank that fails to apply due diligence could find itself unwittingly assisting a corrupt politician to set up nominees and shell companies, ensuring therefore that the beneficial ownership remains hidden. The use of a professional intermediary to open an account on a client's behalf, as related by one expert, can also enable a corrupt public official to open and operate an account virtually anonymously.

37. According to material collected for this year's typologies exercise, anti-money laundering procedures for due diligence and suspicious transaction reporting in FATF jurisdictions generally apply to all banking operations, including private banking, even if most members have not established

[9] Basel Committee on Banking Supervision, *Customer due diligence for banks* (October 2001), p.

specific procedures for this latter category. However, the low numbers of suspicious transaction reports from private bankers and the fact that reports are sometimes not made until a PEP is publicly exposed (for example through the media) as allegedly involved in corruption or other crimes indicates that there still might be a problem. In one example presented during the typologies meeting, an FATF expert described a recent investigation involving a corrupt PEP, USD 70 million in criminal proceeds, and five financial institutions. Two of the institutions were found to have significantly failed to apply appropriate anti-money laundering safeguards concerning PEPs.

38. A failure to apply necessary due diligence in the private banking may simply be because of a lack of knowledge of the family, business or business connections that would indicate a PEP. In this regard, a few contributions to this exercise emphasised that, even if private banking customers are well known, their potential for corruption may not be. It is perhaps relatively easy to name the leaders of countries with a serious official corruption problem; however, it may be more difficult to name other members of the government, senior officials or their family members. Corrupt officials often use their relatives and other associates to launder their illegal obtain funds.

Example 12: Private banker helps conceal suspect's illegal proceeds

The example relates to a merchant bank whose services included institutional brokering, retail brokering, private client services, global equity derivatives, securities, futures and margin lending. Clients of the merchant bank may enter into a private client agreement, which enables the client to perform transactions by telephone or facsimile. During the course of the investigation, difficulty was encountered in matching money coming into the suspect's trust account to any funds that had been sent out of the country by a co-offender. Upon reconstructing the money trail through bank deposit and withdrawal records, it was found that the co-offender had sent an equivalent amount of funds out of the country through international telegraphic transfers; however, the transfer did not record the co-offender as the ordering customer. The ordering customer was recorded in the name of the merchant bank. This provided a way to disguise the remittance of funds offshore.

Example 13: Failure of due diligence aids a potentially corrupt PEP

In Country A, an institution is established whose chairman is also the ruler of that country. This institution is the ordering customer in a payment transaction. Both the ordering customer and the beneficiaries are established in different parts of the world. Neither party is a customer of the bank in Country B.

A bank in Country B is affiliated with the national bank of Country A and is charged with a large part of that country's external payments. Payment is made through the bank in Country B, which acts solely as a correspondent bank for the banks of the ordering customer and the beneficiaries. Due to the lack of adequate due diligence on customers by the ordering institution in Country B (only the respondent has been monitored), the nature, motivation and exact (complete) purpose for the transaction can only be guessed at. These could be either legitimate (many external payments are performed through the Country A bank) or illegal proceeds.

The exact role of Country A's ruler, the beneficiaries of the transactions, the basis for the payment, etc. are not available. This lack of information means that the bank in Country B would not normally be able to determine the significance of the transactions.

Possible remedies

39. While the numbers of suspicious transaction reports from private bankers may be low in some jurisdictions and the thoroughness of due diligence procedures by some private bankers may not yet have reached the same level as for other banking sectors, the compliance culture within private banking may be strengthening. This positive development, according to one FATF member, results from the extensive negative publicity that followed the naming by authorities of the 19 financial institutions involved in the Abacha money laundering scandal in August 2000.

40. Partially in response to the publicity associated with this scandal, 11 international private banks developed and agreed to adhere to special anti-money laundering guidelines known as the

Wolfsberg Principles.[10] The central theme of these guidelines is a more thorough application of know-your-customer rules. The principles also cover such issues as customer acceptance and identification, establishment of beneficial owners for all accounts, due diligence to be performed for normal and high risk customers (particularly, public officials, their families and close associates), the identification of unusual or suspicious transactions and the monitoring of account activity. The principles are not new concepts but rather a means of reinforcing a number of the essential elements of an effective customer due diligence programme.

41. Guidance for dealing with PEPs has also been issued by the Basel Committee on Banking Supervision in its recent publication on due diligence for banks[11]. Additionally, the FATF review of the Forty Recommendations is examining the subject to determine whether refinement of existing measures or the development of new ones is warranted for dealing with identification and due diligence regarding PEPs.

42. While adequate application of existing preventive measures regarding PEPs and funds derived from corruption is essential, the FATF experts brought up another important issue of the action to be taken by authorities that have detected transactions involving such individuals and illegal proceeds. If the individual involved is a high-ranking official in his or her country, it may be impossible to obtain further evidence against the person from other officials of that country. For example, although the national law of most countries contains rules that permit the seizure of assets of illegal origin, international law gives special status to some categories of PEPs. In some instances, the immunity from prosecution that such individuals may hold could prevent a particular jurisdiction from seizing or confiscating their assets.

43. The seizure or blocking of assets of a corrupt foreign political official represents only one phase in an investigation. The jurisdiction holding the assets must then determine to whom the assets will be returned. There is at present no comprehensive international instrument dealing with the process of restitution of seized proceeds or property. Those instruments that do deal with the subject do so from the perspective of specific topics (for example, narcotics trafficking, terrorist financing, organised crime). Although restitution of the seized assets to the country of origin would seem the logical choice, this option is not always possible or appropriate, especially when the country of origin suffers from widespread corruption or misgovernment, or there is the possibility of further embezzlement of the returned assets. Other measures will have to be considered, such as indirect restitution through a third party (an international development bank, for example) or allotting the funds to development programmes or debt relief.

[10] The Wolfsberg Principles is a series of anti-money laundering guidelines jointly agreed to in October 2000 by a group of 11 international banks for their private banking operations. The institutions involved in the development of these guidelines include: ABN Amro Bank NV; Banco Santander Central Hispano, SA; Barclays Bank; Citibank, NA; Credit Suisse Group; Deutsche Bank AG; Goldman Sachs; HSBC; JPMorgan Private Bank; Société Générale; and UBS AG.

[11], Basel Committee on Banking Supervision, *op. cit.*

CHAPTER 4 – BEARER SECURITIES AND OTHER NEGOTIABLE INSTRUMENTS

44. Information developed through the FATF non-cooperative countries and territories (NCCT) initiative shows that bearer securities available in certain jurisdictions represent a particularly useful instrument in the setting up of international money laundering schemes. The bearer cheque is still an important negotiable instrument in use in some regions of the world and could be, along with other types of bearer instruments, another means of laundering criminal proceeds. The purpose for examining this broad subject in this year's typologies exercise was to identify the real vulnerabilities of bearer shares and other financial instruments in bearer form that launderers may be able to exploit.

Bearer securities

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

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

47. With regard to bearer bonds, it should be noted that their use in laundering operations has not yet been documented to the same extent as that of bearer shares. Bearer bonds, according to one FATF expert, have been observed as part of large-scale fraud operations, and the resulting schemes have been reported as suspected money laundering operations. Because of the nature of bearer bonds as debt instruments however, it is possible that their anonymous transferability represents the chief characteristic that could be exploited by launderers rather than an ability to conceal ownership.

Example 14: Bearer shares serve as obstacle to investigation

As a result of a drug importation investigation, approximately USD 1.73 million was restrained in combined assets from residential property and bank accounts. These assets were located in four countries in North America, the Caribbean and Europe. Significant assets restrained involved two offshore companies incorporated in Country A. Investigators also seized original bearer shares of three offshore companies and original articles of incorporation. The investigation revealed that one of the suspects used the services of a lawyer form Country B to design a money laundering scheme that included the incorporation of offshore companies with bearer shares. The lawyer hired the services of a management company in Country C, who in turn used the services of a company in Country A to incorporate bearer share companies in Country A.

There was no requirement to register the names of the shareholders at the corporate registry office, company head office or anywhere else. The only names that appeared were the original incorporators of the company in Country A, who then forwarded the bearer shares and articles of incorporation to the Country B management company. The management company then forwarded the original bearer shares and articles of incorporation to the lawyer, who in turn handed them over

to his client. The files held by the management company only contained the names of the nominee directors, nominee administrators and the directions given by the Country B lawyer who acted on behalf of the suspect shareholder.

The use of bearer shares companies and professional intermediaries in this investigation almost offered absolute anonymity to the person in possession of the bearer shares and is clearly a powerful tool to conceal proceeds of crime. If investigators had not seized the bearer shares in the possession of the suspect, it would have been impossible to determine the owner of these companies and ultimately to identify and restrain their assets as proceeds of crime. In this case, the offshore companies held significant assets alleged to be the proceeds of crime, bank accounts in Country C, and residential property in Country B and Country D.

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

Other bearer instruments

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

Bearer cheques

50. Bearer cheques are unconditional orders (negotiable instruments) that, when presented to a financial institution, must be paid out to the holder of the instrument rather than to a payee specified on the order itself. Bearer cheques are used in a number of countries. The financial institution is usually not obligated to verify the identity of the presenter of a bearer cheque according to international convention[12] unless the transaction exceeds a particular threshold. A non-bearer cheque may become a bearer instrument, payable to the individual who presents it, when the original payee has endorsed it.

Example 15: Money laundering through third-party cheques

The operation began after six STRs were referred to an investigation team. These reports related to the clothing industry and the use of third party cheques in large-scale money laundering and tax evasion activities. Investigations revealed that a cheque casher, operating within an ethnic community, was acting for reputable wholesalers within the clothing industry. However, by cashing cheques through third party bank accounts, evasion of income tax by manufacturers was made possible.

During the operation, a further 13 STRs were identified as being relevant to this investigation. STR information helped identify new accounts and the beneficiaries of the funds being remitted offshore. It was found that the agent involved in the scheme was charging a commission for cashing the cheques through business bank accounts that had been opened for this specific purpose. This operation concluded with the arrest of 27 people, who were convicted and sentenced to terms of imprisonment ranging from 15 months to two and a half years. In total, over USD 7.78 million was laundered and fines imposed amounted to millions of dollars in cash and gold bullion.

[12] Article 5, *Convention on the uniform law of cheques*, Geneva, 19 March 1931.

Travellers' cheques

51. Travellers' cheques are an easily obtained financial instrument that can be carried overseas without requirement to declare their movement. Several FATF members have indicated detecting use of travellers' cheques as an instrument for laundering of funds – either alone or in connection with other bearer instruments. In some instances, these cases have involved purchases (for cash) of large quantities of travellers' cheques. The instruments are used to reduce the bulk of the proceeds for movement overseas, direct purchase of high value items to enrich the individual or as a direct payment for contraband or narcotics.

Example 16: Travellers' cheques provide anonymity for criminal transactions

STR reporting indicates that criminals may be using travellers' cheques as a money laundering tool to provide anonymity to the purchaser and/or the ultimate payee. Although travellers' cheques may be a preferred instrument for conducting large business transactions in some countries, the use of travellers' cheques to negotiate these transactions may offer the opportunity to commingle illicit funds with legitimate funds. Several major banks and travellers' cheque issuers have detected and reported suspicious practices involving the use of hundreds of thousands of dollars worth of activity in travellers' cheques, often in strings of sequentially numbered thousand-dollar cheques. In some cases, the payee was a numbered account in a foreign bank. Frequently, the name and/or address on the purchase agreement were left blank, unverifiable, illegible, or not matching the signature name on the corresponding travellers' cheques.

Two NCCT jurisdictions and a number of East Asian countries have been cited in multiple STRs as the point of origin or negotiation for instruments involved in this type of activity. An example was the purchase of travellers' cheques from an investment house/travel agency in Asia, where the travellers' cheque seller appeared to have gone to unusual lengths to conceal the identity of the buyers. One employee of the travellers' cheque seller personally signed the purchase agreements for USD 27 million worth of travellers' cheques. When the travellers' cheque issuer told the seller to have the buyer sign the purchase agreement, the travellers' cheque seller produced purchase agreements with many different names, but frequent similarities in signatures.

Bank cheques[13] and bank drafts (bills of exchange)

52. The use of bank cheques to move value between persons or jurisdictions is usually not reportable. In most cases, a bank cheque can be issued in any name, and, in many FATF members, identification requirements would not be invoked unless the transaction involved cash or an amount over a specific threshold (or both). A bank draft is a simple variant of cheque used in international payments. They constitute an unconditional written order by one party (the drawer – issuing bank) through which a second party (the drawee – normally the principal correspondent bank of the currency of issue) pays a fixed amount to a named party (the payee). Although not strictly speaking bearer instruments, both of these types cheques have frequently appeared in cases of money laundering alongside other true bearer instruments.

Example 17: Fraud and tax evasion funds moved offshore through purchase of bank cheques

The proceeds of fraud and tax evasion were remitted offshore by purchasing bank drafts in structured amounts and with false sender details and then sending those drafts overseas, where they were deposited in bank accounts under false names. This simple method of moving funds was highly effective (funds exceeding USD 2.6 million were transferred by draft in one 12-month period) and went largely undetected. The ease of the process was aided by the lack of a requirement to produce photographic identification when purchasing the cheques.

Possible remedies

53. Given the limitations of time and the number of topics considered during this year's typologies exercise, there was insufficient time to develop fully the issue of the role of bearer securities and other negotiable instruments in money laundering. FATF experts were however able to agree that there are considerable potential risks of abuse of these mechanisms by launderers, primarily stemming from their ease of transfer and their utility in concealing or disguising ownership of assets.

[13] "Certified" or "registered" cheques in the United States.

54. In the case of bearer shares, it is particularly this last characteristic that poses the greatest problem according to some of the FATF experts. Especially when combined with excessive banking secrecy or other negative features, bearer shares seem to offer a very effective method of hiding the links between a criminal proceeds and the criminal himself. Solutions proposed by the FATF experts for dealing with this vulnerability ranged from eliminating bearer shares altogether to relying on various other already existing controls or measures to work around their lack of transparency.

55. The FATF is currently examining the issue of bearer shares in the framework of its review of the Forty Recommendations. Discussion of this subject is ongoing and is currently focused on the issues raised here along with a more in-depth analysis of the legitimate and illegal uses of such instruments.

CHAPTER 5 - CO-ORDINATED MONEY LAUNDERING AMONG ORGANISED CRIME GROUPS

56. Some FATF jurisdictions have observed that organised crime groups may be working together to co-ordinate their money laundering activities. This co-ordination involves having specific steps of the laundering process handled by different organisations – one group deals with structuring transactions, while another handles the layering step, for example – for proceeds derived from the same crime. Certain of the experts in the FATF-XII typologies meeting mentioned having seen similar activity. This topic was originally proposed for this year's exercise; however, due to the addition of terrorist financing to the agenda for the Wellington meeting, the experts did not discuss it during their meeting. The following material is therefore a short summary of written material submitted by the experts prior to the meeting.

57. FATF members indicated that their investigative authorities were seeing signs of co-ordination among organised crime groups in the area of money laundering, although the nature of and reasons for this co-operation varied. One FATF member noted that the multi-cultural and multi-ethnic nature of its society was contributing to a breakdown in the strict distinctions among organised crime groups along ethnic or national lines. This breakdown has led to an increasing division of labour or specialisation of work – particularly for money laundering – according to economic connections or financial expertise. One of the positive outcomes of this development is the erosion of cultural barriers that often serve as obstacles to investigations.

58. Another FATF member, in describing the co-operation among organised crime groups in its jurisdiction, found that the money laundering function is shared but also is unexpectedly fluid. A group that may launder the funds for another group in one instance may reverse roles and provide its own illegal proceeds to that group for laundering on another occasion. It appears that these joint criminal ventures are more likely to be determined by timing, opportunity and circumstances than any sort of specialisation.

59. An FATF member from another region has also detected co-operation among organised groups and specialisation in the area of money laundering, although the division of labour still appears to be according to differences among traditional organised crime groups. The specialisation in money laundering arises from the fact that laundering operations can be somewhat technical and thus may require specialised knowledge or expertise that may not be available among the rank and file of a traditional criminal syndicate. The authorities in this jurisdiction have furthermore seen signs of certain crime groups that specialise in money laundering and carry out that function for a variety of other, unrelated criminal organisations.

Example 18: Co-ordinated laundering activity by organised crime

In December 2000, following an exhaustive analysis of documents collected during several police operations, law enforcement authorities initiated a pro-active investigation which allowed it to identify some of the organisations involved in collecting and transferring abroad the cash criminal proceeds for various other crime groups.

The organisations allegedly operated through couriers in order to avoid detection and reporting of suspicious transactions. The couriers used by the criminal groups were often members of the same family, and they represented the core link between the customers and the same organisation.

The customers of couriers were allegedly divided into two different groups. The first involved individuals and companies who needed to avoid paying taxes and the banking channels under anti-money laundering monitoring systems. The second group included criminal organisations involved in different criminal activities.

60. Several FATF jurisdictions pointed out that some organised crime groups are able to launder their funds using supposedly legitimate professional services that appear to cater to needs of such groups. Two members described instances of bureaux de change that appear to have provided laundering facilities to various unrelated organised crime groups. A number of other jurisdictions

reported that certain professional financial consultants (for example, civil-law notaries, lawyers, and financial consultancy firms have carried out laundering activities for different organisations without themselves being linked to any specific criminal group. In some cases, these service providers may not have known the criminal nature of the proceeds they helped to move or conceal; however, others entered into this work fully knowing the illegal origin of the funds concerned.

CHAPTER 6 – INTRODUCTION OF EURO BANKNOTES

61. Euro banknotes and coins were introduced in the twelve Eurozone members on 1 January 2002, following a three-year period during which the euro currency existed only in electronic form. The FATF originally examined the money laundering implications of euro introduction during its 1998-1999 typologies exercise. At that time, it concluded that any potential money laundering risks would likely be tied to the introduction of the new currency in physical form and the subsequent phase out of the national legacy currencies in the period leading up to and following January 2002. This topic was proposed for this year's typologies exercise as a follow up to the earlier FATF work on the subject. However, again due to the addition of terrorist financing to the agenda for the Wellington meeting, the experts did not discuss this topic during their meeting. A summary of written material submitted by the experts follows.

62. FATF members (from both within and outside the Eurozone) and the European Central Bank acknowledged that there was a potential threat of money laundering during the introduction of the euro in physical form. The specific vulnerabilities mentioned were transactions involving cash in Eurozone legacy currencies exchanged for the new physical euros, transactions involving occasional customers and structured transactions.

63. Among the Eurozone members that contributed information on this subject, it was universally accepted that the current anti-money laundering systems were adequate to detect any attempts to use the physical euro introduction to conceal laundering operations. No Eurozone members appear to have changed their anti-money laundering legislation specifically in response to the physical changeover. Virtually all Eurozone members did make policies during this time of strict adherence to and application of current measures with, in many cases, intensification or refinement of certain procedures.

64. Almost all Eurozone (and EU members outside the Eurozone) reported having established policies increasing awareness at financial institutions of the potential risks of money laundering in the period leading up to the physical changeover. Sometimes this was incorporated in a larger programme to sensitise the financial sector on other security risks during the period (for example, the possibility of increased risk for currency transport, attempts at counterfeiting and fraud). Along with this increased awareness for financial institutions, some Eurozone members required that financial institutions emphasise anti-money laundering procedures and policies in personnel training during this time leading up to 1 January 2002.

65. Another measure taken in some Eurozone members was to encourage the public directly or through financial institutions to make cash deposits of national currencies prior to 31 December 2001 and then to rely on non-cash transactions (debit and credit cards, for example) after the start of the year. Even minor a reduction in the volume of work after the 1 January would enable personnel at financial institutions to have a better overview of any potential abuses for money laundering.

66. Several Eurozone members also focused on customer identification and "know-your-customer" aspects in increasing anti-money laundering vigilance during the changeover period. Certain of the jurisdictions suggested that financial institutions encourage their customers to go to the branch where they are already known. Cash transactions by occasional customers were therefore to be discouraged. An additional measure to reinforce this point was taken by Eurozone members in lowering the threshold amount requiring identification of occasional customers (in one case, for certain types of transactions, it was set as low as EUR 635).[14]

[14] European Council Directive 91/308/EEC requires that occasional customers conducting transactions of EUR 15,000 or more be identified by the financial institutions.

67. Finally, certain Eurozone members stressed strict application of suspicious or unusual transaction reporting obligations during the changeover to the physical euro. This reporting was to be supplemented in at least one member by reporting to the financial intelligence unit (FIU) of any cash transaction over a EUR 30,000 threshold and in another member by urging that financial institutions report their suspicions to the FIU more rapidly.

68. Only two of the Eurozone members that provided written material for this typologies exercise reported increased numbers of suspicious or unusual transaction reports that may have been attributable to the changeover to the physical euro. There was a notable increase in STRs related to exchange operations in the period leading up to the change over. In one instance, an FATF member indicated that a very high proportion of its STRs for the last year had involved bureaux de change, for example. However, there is presently no clear evidence that this increase is directly related to the introduction of the physical euro. all other participating Eurozone members observed no increase in STRs that could be directly related to the changeover.[15]

69. Two European Union members that have not yet joined the Eurozone (and contributed to this exercise) likewise were not able to point to a significant increase in suspicious exchanges that could be potentially related to the euro changeover. Only two non-European FATF members submitted material on the subject. Both had observed a recent increase in the number of exchange transactions relating to their currencies and those of the Eurozone. However, neither jurisdiction was able draw conclusions as to whether any of this activity involved potential money laundering.

70. Eurozone members have confronted potential money laundering risks arising from the introduction of the euro in banknote and coin form by relying on and re-emphasising anti-money laundering measures currently in force at the national level. Although there was a certain degree of co-ordination at the European level regarding specific measures to be implemented during the changeover, this co-ordination did not result in a uniform response from all Eurozone members. There have been some common features of the initiatives taken up by Eurozone members: the focus on increasing awareness of money laundering risks and of rules and obligations for financial institutions, for example. However, individual members decided in what manner and to what degree to enhance or focus their anti-money laundering programmes during this time.

[15] Several members also noted overall increases in suspicious and unusual transaction reporting during the fourth quarter of 2001, largely because of the September 11th events.

CHAPTER 7 – SUSPICIOUS TRANSACTION REPORTS & MONEY LAUNDERING CASES

71. As an additional focus of this year's typologies exercise, the FATF looked at money laundering cases as they are derived from or contributed to by suspicious or unusual transaction reports (STRs). The goal of discussion of this topic was to highlight the important role that STRs have in the fight against money laundering. FATF members were asked to provide examples of three types of money laundering cases: (1) money laundering cases derived directly from STRs, (2) money laundering cases that were not directly derived from STRs but which received significant contributions from STRs and (3) money laundering cases developed from other sources and in which STRs played no role.

The role of STRs in anti-money laundering investigations

72. Suspicious or unusual transaction reports (STRs) have a key function in the overall anti-money laundering programmes of individual FATF members. This function is either to generate anti-money laundering cases or to contribute to the successful outcome of such investigations. Within FATF member jurisdictions, it appears that by far the majority of investigated or prosecuted money laundering cases are related in some way to STRs (again, either derived from or supplemented by STRs). In those members where STRs serve as the direct source of the cases, the proportion of non-STR related cases seems to be small (some experts mentioned figures ranging from none to five or ten percent).

73. For those countries in which the STR serves as a supplemental source of information, the proportion of non-STR cases is perhaps higher. Moreover, the nature of the cases differs from those generated by STRs. In a number of jurisdictions, money laundering investigations do not really occur independently of the predicate offence that may have produced illegal proceeds. For example, one FATF member stated that most of its cases with money laundering aspects arise as part of narcotics or, more recently, terrorism investigations. Any investigation or prosecution for the money laundering offence occurs only in conjunction with the main predicate offence. This finding is also reflected in the written materials on this subject supplied as part of this year's exercise. STRs are thus used to help establish links to other parts of the criminal operation. It would seem to be true as well that money laundering cases with no links to STRs also come from similar types of investigations; however, money laundering cases without any links to STRs are increasingly rare.

Example 19: Exchange transaction leads to case of laundered drug and diamond smuggling proceeds

A foreign exchange transaction of a European currency into US dollars for a value of almost USD 177,000 was reported to the FIU of an FATF member jurisdiction (Country A). At the time of the transaction, the individual, of Asian origin, gave the exchange office an address in another FATF country (Country B). This first transaction was soon followed by four more similar transactions. After several weeks, the total had already attained USD 618,000. After a break of six months, the exchange transactions resumed. Over a four-month period, the intermediary appeared with large amounts in pesetas to be converted into dollars. The total amount of the transactions described in reports to the FIU amounted to more than USD 1.3 million.

The information obtained from law enforcement demonstrated that the individual had no criminal record in Country A. Given that the case involved large amounts for which there existed no apparently legitimate economic justification, the FIU pursued the investigation. Several foreign FIUs were queried. One of them was able to provide useful information: the individual was known as a member of a group of drug traffickers who performed the same type of transactions in the country involved. Investigations of the members of this group was already in progress in this latter country. Secondly, it appeared that the address provided during the first contact with the financial institution was false. On the basis of these elements, the FIU decided to turn over the case file to the prosecutorial authority.

The subsequent investigation showed that the individual had not been not acting alone. For a number of years she had played a dominant role in money laundering transactions involving a total amount of around USD 11.5 million. The individual was arrested in the company of one of her accomplices and in possession of a large sum in dollars. She acknowledged the retail foreign exchange transactions, as well as the illicit origin of the funds. According to her account, they were derived from illegal diamond trafficking. She was sentenced to four years in prison (two of which were

suspended) and a fine of nearly USD 1 million. The funds seized were confiscated, as well as the amounts exchanged; her accomplices were each sentenced to two years in prison (one of which was suspended).

This example clearly illustrates the importance of international co-operation and the exchange of information between FIUs and their foreign counterparts in the detection of money laundering transactions. It also demonstrates the necessity for the financial institutions to continue sending suspicious transaction reports to the FIU, even when they do not at first seem to produce an immediate response from the authorities.

Example 20: Investigation of human being trafficking aided by STRs

This case involved the laundering of human being trafficking proceeds from the three FATF jurisdictions (Countries C, D and E) through another FATF jurisdiction (Country F) to an Asian country (Country G). In the space of 2 years, proceeds totalling USD 148 million passed through over 70 accounts in Country F. The proceeds were remitted from illegal immigrants in the three jurisdictions to bank accounts in Country F before they were sent to the organisers of the trafficking ring in Country G through an underground banking system involving over 50 different remittance agents. Only two of these remittance agents were properly registered under applicable national regulations. The unregistered ones naturally did not keep any records of the transactions. The two registered ones kept records in accordance with the law since registering but not before.

The operation began following the receipt of information from law enforcement authorities in Countries C and D concerning the receipt of what they believed to be proceeds of human being trafficking by the same people in Country F. After to a co-ordinated operation in the three jurisdictions a link to Country E, which was also believed to involve illegal immigrants returning funds to Country G, was discovered.

In Country F six people, including a family of five, were arrested for money laundering and other offences, in relation to the moving of the funds from overseas through Country F to Country G. During investigations 18 STRs related to the main targets and the remittance agents were of great assistance in regard to identifying accounts and fund flows. Previously these STRs had only been indexed and filed.

Example 21: Proceeds from bank hold up laundered through bookmakers, no STRs filed

Two serious armed robberies occurred in which approximately USD 1.9 million was taken. During police investigations into the armed robbers themselves, it came to light that another individual had been placing a vast number of bets in a number of bookmakers within one city. While this in itself is not unusual or even suspicious, it was noted that he always followed a similar pattern whereby the stakes were high and the odds low. In other words, he bet on "favourites" who were likely to win, although this likelihood meant that the sum received by the bet maker if he did win was relatively small. Consequently, he made a 7% net loss over a long period of time. This would be quite a serious loss for a professional gambler. Further enquiries into this individual revealed that he never received his winnings personally, but had cheques made out to a total of 14 different bank accounts in the names of 10 third parties. This ensured that the receipt of money never raised suspicions within the banks and other financial institutions utilised, because no one will question the odd cheque from a bookmaker. However, the suspicions of the investigators were confirmed when it was discovered that several of the cheques were issued in the names of the armed robbers and their immediate families. The link between the money launderer and the original criminals was established. The former was convicted of money laundering and sentenced to 5 years imprisonment. He had laundered approximately USD 3.3 million through this system.

74. The number of STRs received by individual FIUs in FATF member jurisdictions appears to be growing. Although banks would be expected to be the primary source of such reports within a particular jurisdiction, this is not always the case. In a few jurisdictions, the number of reports originating from other types of financial institutions – especially for bureaux de change – seems to have well outstripped the reporting from banks. It is difficult to say why the overall reporting is increasing; however it is probably safe to say that it is due primarily to increased awareness of reporting obligations within a particular sector. A sharp rise can sometimes be attributed to a particular information campaign or other unrelated factor. For example, several experts stated that there had been an immediate increase in STRs following the September 11th terrorist attacks in the United States and through the publication of lists of terrorist suspects.

75. The tendency, as anti-money laundering programmes evolve, for additional financial services or other entities to fall under anti-money laundering rules and procedures logically also increases the number of STRs. FATF experts believed that applying such measures to new areas as appropriate was a positive factor in further enhancing anti-money laundering systems. However, they also expressed some concern that there is not at present a consistent approach by FATF members in applying anti-money laundering measures beyond a core group of financial institutions to categories of businesses or individuals that also often facilitate money laundering such as to non-financial professionals, casinos and other gaming ventures, etc.

76. A common theme in earlier typologies exercises has been the instrumental role that non-financial professions – such as lawyers/notaries, accountants, etc. – play in setting up or facilitating complex money laundering schemes. FATF experts in this year's exercise stressed the urgent need to bring the non-financial professionals, when performing particular functions under the same anti-money laundering rules as for other financial services. It was noted that some jurisdictions already apply requirements to certain legal and accounting professionals.[16] However, it appears that even when subject to anti-money laundering rules, the non-financial professions still display an unwillingness to co-operate with anti-money laundering authorities in contrast to the relationship that exists in most jurisdictions between these authorities and the financial sector. This fact is especially reflected in the generally low number of STRs submitted by this group. One of the experts mentioned that the legal and accounting professions often cite concerns about confidentiality or the fear of losing a client as the reason for not wishing to be subject to STR requirements. However, according to this expert, their unwillingness to participate fully in the anti-money laundering process may have as much to do with the lack of public pressure for them to do so.

Example 22: Lawyer fails to file STR

"L" was a solicitor practising in an FATF jurisdiction. A client indicated to "L" that he wanted to deposit a sum of money into his trust account. This was agreed to and the sum of USD 15,000 taken to his office, counted, receipted and subsequently deposited in his trust account. A short time later this process was repeated with a further USD 184,000 deposited. A week later the process was repeated but, on this occasion, the sum was nearly USD 37,000. The following day the total amount of USD 67,000 was disbursed through a mortgage payment by direct credit to a bank and a further payment of USD 59,000 direct payment to the client's estranged wife.

The bank that had received the initial three deposits made suspicious transaction reports to the FIU, based on a concern over the amount and that this was largely made up of a single denomination of banknotes. Representatives from the national bar association subsequently spoke to "L" concerning the deposits. "L" expressed the view that it was the responsibility of the financial institution to submit STRs to the FIU under the anti-money laundering law and that he was therefore not required to do so. After his meetings with the bar association investigators, "L" reported the transactions to the FIU.

Law enforcement investigators later searched "L's" office as part of a money laundering investigation tied to drug trafficking offences allegedly carried out by his client. "L" was later charged under anti-money laundering legislation with failing to file suspicious transaction reports. In his defence, "L" claimed to have held no suspicions in relation to the deposits and supported his claim with various references to the known financial affairs of his client.

In deciding this case, the judicial authorities stated that ignorance of the existence of the legal obligation to report was not a defence to this charge. It also found that transactions involved in this case lacked any credible explanation and that they must have been relevant to the investigation or prosecution of a money laundering offence. "L" was subsequently convicted for failing to report the transactions.

[16] Changes made in December 2001 to the European Council Directive on money laundering (91/308/EEC) now place "notaries and other independent legal professionals", as well as "accountants and auditors", in the list of legal or natural persons which should be subject to anti-money laundering obligations, including the reporting of STRs. The Directive must be implemented in EU member States by 15 June 2003.

Example 23: Complex money laundering scheme revealed and monitored through STRs

An STR was received from a large commercial bank giving details of unusual behaviour in a business account. While initially happy to accept the business, the bank later became suspicious due to the nature of transactions on the account and the behaviour of the account holder. It closed the account and simultaneously submitted an STR.

This individual report appeared to be fairly innocuous; however, when more STRs were received on the same suspect from a number of different sources, an investigation was initiated. The STRs were compiled and a more comprehensive analytical product was developed and disseminated to law enforcement. The investigation revealed that a foreign bank operating in the country had been defrauded of over USD 576,000 by a former employee.

The STRs built up the picture of how this illicit money had been and was to be laundered. The initial STR had in fact been made on a company account for one of several front companies set up by the suspect. Funds had been placed into these accounts specifically to ensure successful placement and layering. Law enforcement were then also able to identify other business accounts set up for the same reason.

Further STRs were received from several casinos. They had become suspicious after repeatedly being asked to cash bank drafts for up to USD 28,000. These would be held by the casinos in order for the suspect to bet against. When the evening's entertainment was over, any winnings as well as the remaining deposit would be withdrawn and replaced into different bank and building society accounts.

The number of STRs and suspicion surrounding the criminal and his associates meant that law enforcement closely monitored any financial transactions that they made. This ensured that a third method of laundering was discovered. The criminal had a foreign exchange business in an offshore centre. Some of the illicit funds were placed into this business, perhaps in the hope that it would be more difficult to trace.

The structure of the Suspicious Transaction Reporting System enabled two criminals to be caught, up to half of the defrauded money to be reclaimed and a laundering methods to be identified. The criminal has since been arrested and charged with conspiracy to defraud and theft, as well as money laundering, and awaits trial.

Quantity vs. quality

77. A perennial issue for authorities receiving STRs is finding ways to deal with increasing numbers of reports but doing so with a fixed number of analytical or investigative personnel. The solution in several FIUs, according to some FATF experts, is to focus on fewer, more important cases and to strive for more rapid but higher quality products for the "end-user", whether that be prosecutorial/ judicial authorities or an investigative agency. At present, there does not appear to be a standard as far as the desired "percentage" or portion of STRs that should eventually go to the end user. The numbers obviously may vary according to whether STRs are the primary source of money laundering investigations as indicated above. One FATF member stated that about 25% of all STRs received by his FIU go on to prosecutorial authorities. Another mentioned that essentially all STRs are investigated in his jurisdiction because of the nature of the FIU as a police authority. Still another expert stated that it is impossible to determine the number of STRs that are ultimately used in prosecutions or investigations since these reports are used in her jurisdiction as a resource for supplementing ongoing financial investigations.

78. Statistics provided by FATF experts as part of the discussion of this topic also appear to further illustrate the varying roles that STRs play in different anti-money laundering systems. Certain FATF members had moderate numbers of STRs for a given period but a relatively high number of convictions for the money laundering offence. Other jurisdictions had higher numbers of STRs but showed relatively lower numbers of convictions. Several factors could be at play here. As mentioned above, the nature of the anti-money laundering system could be such that the STR represents the principal source of money laundering investigations, while in others the STR serves primarily as a supplemental source of information for law enforcement investigations. In the first type of system, it is usually possible to trace the STR from its inception through the analysis process to any prosecutions/investigations and eventual convictions that may follow from it. In the latter type of system, it is not always possible to relate individual STRs to specific outcomes, especially if money laundering is not usually investigated or prosecuted independently from other charges.

Money laundering methods, trends and guidance

79. Increasingly, STRs are becoming a primary source of information for the development of various other products that indirectly contribute to money laundering case analysis or investigation. The use of STRs in helping to identify money laundering methods, trends and patterns within particular jurisdictions has been mentioned in earlier years. This function seems to grow more important each year as FIUs and other relevant authorities attempt to understand not only the current state of money laundering techniques and mechanisms but also the effect that anti-money laundering measures are having on them. As one FATF expert indicated, STRs also validate the findings of law enforcement investigations as well as identifying new trends. In many cases, STRs also indicate the presence of certain types of laundering activity in a given area even when the report might not be able to be used to initiate or support a particular investigation.

80. STRs also play a growing role as one basis for developing guidance that financial institutions and others can use as assistance in identifying suspicious or unusual financial activity. When combined with information from actual money laundering investigations, this material is critical in establishing indicators of what should be reported in the future. Several FATF members have produced such guidance and have then circulated it to the end users through financial regulatory agencies or published the material elsewhere.

Example 24: STRs help define problem of loan-sharking

Due to its pervasiveness both throughout the country and across different economic sectors, law enforcement agencies are particularly committed to investigate and stop loan-sharking related offences. An effective contribution to this effort has been provided by the STR system. STRs have been instrumental in bringing about the indictment and prosecution of several physical and legal persons involved in such activity, and at the same time huge sums used for funding it have been seized. Moreover, STRs provide an additional channel whereby the actual dimension of the phenomenon can be defined, thus also offering an effective tool for its analysis.

To this end, thanks to the large number of STRs related to loan sharking that financial intermediaries have processed and to the findings emerging from law enforcement agencies' investigations, a typology has been developed that shows banking behavioural patterns of a loan shark. It may be used then to help identify loan sharking related banking activity. The typology contains the following factors:

- individual profile:
- banking activity inconsistent with the economic profile of its holder and with his/her occupation;
- transactions carried out on a wide range of current accounts, held in the name of different individuals;
- outflow of funds to individuals in dire financial conditions and in occupational fields not linked to that of the account holder;
- account activity profile:
- conspicuous bank activity, mainly amounts credited to the account;
- payments of cash, cheques and bills with round figures, below USD 10,000, where the issuers of the cheques are the same as the beneficiaries of cheques issued by the account holder;
- cash withdrawals taking place at the same time as the deposit of cheques into the account;
- cheques which are issued without the indication of the beneficiary and which are cashed after many different endorsements;
- short time span between the dates of the cheques issued by the account holder and the dates of the cheques deposited into the account, with a spread benefiting the account holder;
- cheques deposited into the account either remain unpaid or are withdrawn before maturity or are eventually paid by a lawyer;
- funds from the account are rarely further invested in financial instruments.

CONCLUSION

81. This report opened with an examination of terrorist financing, a subject that has come to the forefront of FATF work after the September 11th terrorist attacks in the United States and the subsequent change in the FATF remit. Despite being a late addition to this year's typologies exercise, FATF members were able to gather substantial material that allowed a productive discussion of methods used for the funding of terrorism and the ways in which terrorist organisations attempt to use formal and informal financial networks. Terrorist funding is generated from both illegal activities and, unlike organised crime, lawful sources; however, the principal techniques and mechanisms used by terrorists to transfer funds or conceal connections to their sources vary little from those used by criminal organisations. Some members have begun identifying certain characteristics of financial transactions related to terrorism, and these are being used in the development of guidance specifically designed to assist financial institutions in identifying and reporting such activity.[17]

82. The role that correspondent banking relationships play in facilitating certain money laundering schemes is a complex issue. In looking at this topic in this year's exercise, FATF experts found that there are certain vulnerabilities in such relationships that may be exploited by those wishing to access the legitimate financial networks and at the same time conceal their identities or the true nature of their activities. Especially in instances where a respondent bank serves as a correspondent for other financial institutions, there is the risk that the last correspondent bank may not be able to tell on whose behalf it may be carrying out financial transactions. FATF members provided examples of how correspondent relationships may be misused, and the examples appear to show that it is not just a problem for certain jurisdictions. The correspondent banking issues related to customer identification are being considered in the framework of the FATF review of the Forty Recommendations; however, it may be worthwhile developing further case examples in the work of future typologies exercises.

83. Private banking has been characterised in the recent past as being particularly vulnerable to laundering by certain high-profile criminals, in particular politically exposed persons (PEPs). Although PEPs were discussed at some length during the typologies exercise, it should be noted that these individuals are not the only ones who may attempt to use private banking services to conceal their illegal financial activities. Vulnerabilities in this sector may be due inadequate due diligence policies or procedures with regard to high net worth customers. A few experts indicated that there is nevertheless a fundamental difficulty for financial institutions to identify PEPs easily. Various international efforts are beginning to address these issues, particularly the Basel Committee on Banking Supervision and the Wolfsberg Group, and the FATF is likewise looking at the relevant issues in the review of the Forty Recommendations.

84. Regarding bearer securities and other negotiable instruments, it appears that the general ease of transferability and the ability to conceal ownership are the primary characteristics that make such instruments attractive to money launderers. The use of bearer shares to conceal ownership, according to some FATF experts, is a key obstacle to investigating some complex money laundering schemes, especially when there is involvement of non-cooperative countries or territories (NCCTs). The use of other bearer instruments – bearer and third-party cheques, as well as travellers' cheques, for example – has often been observed as part of large-scale money laundering operations. However, their use in such schemes seems to rely on their lack of traceability rather than an ability to obscure connections between a legal entity and its beneficial owners. As with the two previously mentioned topics, the FATF is examining the role of bearer securities as part of the review of the Forty Recommendations.

85. Two other topics were originally planned for the FATF-XIII typologies exercise: co-ordination of money laundering among organised crime groups and a follow-up to introduction of the

[17] As stated under this chapter heading, this guidance is currently in development and will be published by the FATF in due course.

euro. Because of changes in this year's programme however, the FATF experts were unable to discuss these issues during the Wellington meeting. This report thus presents brief summaries of the material that was submitted by FATF members. From this information, it was still possible to highlight some key points. With regard to co-ordination of money laundering among organised crime groups, FATF members have observed cases of this, including a division of labour that does not always follow traditional divisions between groups. It may be useful for relevant authorities to continue looking for additional evidence of this criminal activity.

86. As for the follow-up on introduction of the euro,[18] the primary focus this exercise was to determine whether there were signs that the introduction of the euro in physical form is being used as a mechanism for laundering illegal proceeds. Eurozone members have re-emphasised and enhanced existing anti-money laundering measures to deal with the perceived risk of money laundering during the transition phase (that is, prior to 1 January 2002 and up to mid 2002). No clear trend of increased laundering activity related to the introduction of the euro banknotes and coins has been detected yet.

87. Finally, the FATF attempted for the first time to analyse in some detail the relationship between suspicious or unusual transaction reports and money laundering cases. FATF members provided a significant amount of material that shows both the differing approaches of in anti-money laundering systems and the different stages of their evolution. This material and the related discussions in Wellington demonstrate that STRs play an instrumental role not only in generating money laundering cases but also in supplementing or linking them to other illegal activities. STRs also seem to serve as a further indicator of gaps in anti-money laundering systems. For example, the FATF experts mentioned the need to extend consistent and mandatory reporting requirements for certain sectors, in particular such non-financial professions as lawyers/notaries and accountants. STRs have an important indirect case support role in helping to define money laundering trends and patterns or in developing guidelines for financial institutions. In regard to this last point, it may be worth considering if the focus of FATF typologies work could be directed toward the producing more information in the form of guidance for additional areas (similar to what has been developed for terrorist financing).

[18] See the *FATF 1998-1999 Report on Money Laundering Typologies*, 10 February 1999, available through the FATF website at: http://www.fatf-gafi.org/FATDocs_en.htm#Trends.