Financial Action Task Force on Money Laundering

Groupe d'action financière sur le blanchiment de capitaux

Report on Money Laundering and Terrorist Financing Typologies 2003-2004

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

Contact@fatf-gafi.org

TY2004_en
01.03.2004//15h00

TABLE OF CONTENTS

LIST OF CASE EXAMPLES

EXECUTIVE SUMMARY

1. FATF members, non-FATF members and international organisations attended the 2003 – 2004 typologies exercise providing a global perspective on current money laundering and terrorist financing trends. This year's exercise focused on the following topics: Wire transfers and non-profit organisations (NPOs) and their links to terrorist financing, the vulnerabilities of the insurance sector to money laundering, politically exposed persons (PEPs) and gatekeepers.

2. Wire transfers are a fast and efficient way of moving funds, thus they can also be used for terrorist purposes. Complex wire transfer schemes can be used to create a deliberately confusing audit trail to disguise the source and destination of funds destined for terrorist use. Currently, there a limited number of indicators to help identify potential terrorist wire transfers – primarily the source and destination of the funds and the names of the individuals involved when this information is available. It was acknowledged during this year's exercise that there was a need to identify further information to develop potentially suspicious transactions.

3. The examination of terrorist misuse of NPOs found that the diversion of a very small volume of the funds can represent a potentially serious terrorist financing problem. Various categories of non-profit organisations were recognised, and within each category an associated set of risk profiles began to be identified. Although most governments have some kind of regulation and oversight of the NPO sector, additional measures are likely to be necessary to reduce the misuse within the sector. The experts concluded that there was a need to develop and enhance mechanisms and gateways for information sharing to counter the terrorist financing risk.

4. A number of vulnerabilities to money laundering across the sectors that make up the insurance industry were confirmed. Inconsistent regulation of the industry may provide an opportunity that could be exploited by money launderers. In general, however, the industry is viewed to be most vulnerable at the integration stage of the money laundering cycle. It was observed that there is a low detection of money laundering in comparison to the size of the industry as a whole. This observation will likely require further investigation to develop a better understanding of the specific money laundering risks in each of the different sectors that make up the industry.

5. PEPs are individuals who are or have been in the past entrusted prominent public functions in a particular country. New revelations of suspected PEPs' involvement in financial crime – especially as related to corruption – occur frequently in the press. PEPs, when involved in criminal activity, often conceal their illicit assets through networks of shell companies and off-shore banks located outside the PEPs country of origin. PEPs were noted as frequently using middlemen or family members to move or hold assets on their behalf. The techniques used by PEPs to hide assets are similar to those of money launderers. Financial institutions may thus be able to detect potential illegal activity of PEPs by applying enhanced due diligence methods similar to those used for countering money laundering.

6. Increasingly, money launderers seek out the advice or services of specialised professionals to help facilitate their financial operations. This trend toward the involvement of various legal and financial experts, or gatekeepers, in money laundering schemes has been documented previously by the FATF and appears to continue today. The work undertaken during this year's exercise confirmed and expanded the FATF's understanding of specific characteristics of this sector and what makes it vulnerable to money laundering. A key conclusion of the experts was that many of the risks and vulnerabilities identified for gatekeepers could be reduced if AML/CFT measures were consistently and thoroughly applied.

INTRODUCTION

7. Money laundering and terrorist financing are two types of financial crime with devastating effects that go beyond seemingly innocuous financial transactions. From the profits of the low-level narcotics trafficker to the assets looted from State coffers by dishonest government officials, criminal proceeds have the power to corrupt and ultimately destabilise communities or whole national economies. Terrorist networks are able to carry out their insidious activity – on a global scale and in places that could once be considered immune to such phenomena – through their undetected financial support structures. In both instances, criminals or terrorists are able to exploit loopholes or other weaknesses in the legitimate financial system to launder criminal proceeds and to support terrorist activity.

8. The Financial Action Task Force (FATF) holds an annual exercise to examine the methods and trends – the typologies – of money laundering and, since 2001, of terrorist financing. The primary objective of this work is to obtain material that will help the FATF policy makers develop and refine anti-money laundering and counter-terrorist financing (AML/CFT) standards. In addition, the findings obtained from the annual exercise serve as the basis for informing a wider audience – regulatory authorities, law enforcement agencies and financial intelligence units (FIUs), as well as the general public – on the characteristics and trends of money laundering and terrorist financing.

9. The annual FATF typologies exercise culminates in a meeting of experts. This year's meeting took place from 17 to 18 November 2003 in Oaxaca, Mexico, and was chaired by Mrs. María de la Concepción Patiño Cestafe, Head of the *Dirección General Adjunta de Investigación de Operaciones (DGAIO)*, the Mexican FIU. Taking part in the experts' meeting were 35 countries and jurisdictions, including representatives from FATF members: Argentina; Australia: Austria; Belgium; Brazil; Canada; Denmark; France; Germany; the Gulf Co-operation Council; Hong Kong, China; Italy; Japan; Luxembourg; Mexico; the Kingdom of the Netherlands; New Zealand; Norway; Portugal; Singapore; South Africa, Spain; Sweden; Switzerland; the United Kingdom; and the United States. Also present at the meeting were representatives of the FATF-style regional bodies: the Asia Pacific Group on money laundering (APG, with representatives from Korea, India and the APG Secretariat), the Caribbean Financial Action Task Force (CFATF, with representatives from the Bahamas, El Salvador, Guatemala, Honduras, Panama and Venezuela), the Financial Action Task Force on Money Laundering in South America (GAFISUD), and the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL, with a representatives from Monaco, Romania and the Ukraine). The following observer organisations also sent representatives: the Egmont Group, Europol, the International Monetary Fund (IMF), the International Association of Insurance Supervisors (IAIS), the International Organisation of Securities Commissions (IOSCO), Interpol, the Offshore Group of Banking Supervisors (OGBS), the Organisation of American States (OAS) and the World Bank.

10. Each year, the FATF typologies exercise focuses on a series of topics or themes that were agreed to by the FATF Plenary. The Plenary attempts to select topics according to the current work of the body or to follow up on methods or trends identified in previous typologies exercises. Five topics were therefore chosen for this year. Examining the terrorist financing links with wire transfers and these same links with non-profit organisations (NPOs) were two of the topics of the FATF-XV exercise. They follow up on earlier typologies work, as well as provide material to support further refinement of the guidance issued by the FATF for the Eight Special Recommendations on terrorist financing. The vulnerabilities of the insurance sector to money laundering, the third topic, was selected to build on initial findings from earlier FATF typologies work. Finally, the FATF looked at the money laundering risks associated with politically exposed persons (PEPs) and with specialised financial advice providers or "gatekeepers" as the last two topics. With the issue of the revised FATF Forty Recommendations in June 2003, there are now measures that apply with respect to PEPs and gatekeepers; therefore, this year's typologies work was intended to provide additional information on the nature and scope of the threat for these two areas.

11. Unlike previous years, the typologies exercise for FATF-XV used a slightly different formula for its experts meeting. For three of the topics – wire transfers, NPOs and insurance sector vulnerabilities – a certain amount of work was done in small groups before the experts' meeting in order to bring greater focus to discussions of the topics. Then during the experts' meeting, a smaller break out session (consisting of about 30 operational and policy making personnel) was held for each of the three topics to determine relevant trends and examine any policy implications arising from discussion of the identified typologies. The findings of the three workshops were then presented in the full meeting of experts where they were further debated along with presentations on PEPs and gatekeepers.

12. This report on the FATF-XV typologies exercise describes key conclusions for each of the subject areas as they have been developed from the three workshops, the general meeting of experts and the written material provided by participating delegations before the meeting. As is the usual practice of the FATF, the report includes case examples taken from the written contributions and presentations made during the meeting. The texts of these examples are reproduced here – wherever possible – as they were submitted for the exercise. However, country names, currencies and certain other details have been modified in order to protect sensitive aspects of any cases cited here.

I: WIRE TRANSFERS AND THEIR RELATION TO TERRORIST FINANCING

13. Terrorists use wire transfers to move funds intended for the financing of their activities. The financial support structure revealed after the September 11th attacks in the United States showed the essential role played by wire transfers in providing the hijackers with necessary financial means to plan for and eventually carry out their attacks.[1] It was this use of wire transfers that the FATF had in mind when it issued Special Recommendation VII in October 2001. In order to consolidate information on the characteristics and role of wire transfers in terrorist financing, the FATF chose this as the focus for the first of the workshops held during this year's meeting of experts on typologies.

14. When the FATF uses the term *wire* or *funds transfer*, it is referring to any financial transaction carried out for a person through a financial institution by electronic means with a view to making an amount of money available to a person at another financial institution. In some cases, the sender and receiver could be the same person.[2] Wire transfers include transactions that occur within the national boundaries of a country or from one country to another. Given that wire transfers do not involve the actual movement of currency, they are a rapid and secure method for transferring value from one location to another.

15. Payment systems at both inter-bank and retail level now provide better coverage and efficiency for both domestic and cross-border wire transfers. The continuing development of world-wide networks such as SWIFT has enhanced the reliability and efficiency of inter-bank payment systems allowing a large number of transactions to be processed daily. Within the retail banking sector, services such as telephone and internet banking allowing customers to execute transactions on a non face-to-face basis from any location with telephone or internet access.

16. Advances in payment system technology have had a twofold impact in relation to the potential abuse by terrorist financiers and money launderers of such systems. On the one hand, electronic payment systems provide greater security for transactions by permitting an increased ability to trace individual transactions through electronic records that may be automatically generated, maintained and/or transmitted with the transaction. On the other hand, these advances also create characteristics that may be attractive to a potential terrorist or money launderer. For instance, the increased rapidity and volume of wire transfers, along with the lack of consistent approach in recording key information on such transactions, in maintaining records of them and in transmitting necessary information with the transactions, serve as an obstacle to ensure traceability by investigative authorities of individual transactions.

17. A further complication is presented by transfers that take place through non-bank financial institutions such as money remitters, bureaux de change or other similar types of businesses. In some countries, these businesses perform wire transfer functions either directly with counterpart businesses in their own country or abroad or else through conventional financial institutions (i.e. banks). Again, differences in requirements for recordkeeping or transmission of information on the originator of transfers conducted through such businesses may be used to the advantage of terrorist or other criminals that desire to move funds without being easily detected by authorities.

Typologies

18. The FATF experts recognised that wire transfers are a fast and efficient way of moving funds for terrorist purposes. For example, a simple network for transmitting terrorist funding can be set up merely by taking advantage of the differences in the monitoring regimes of various countries. If no records on the originator of the transaction are kept at the starting point of the wire, or the information

[1] See the statement of Federal Bureau of Investigation to the US Congress, which was cited in last year's FATF report and is available from http://www.fbi.gov/congress/congress02/lormel021202.htm. The statement contains financial profiles of the September 11th hijackers and mentions the use of wire transfers for moving funds.
[2] See Interpretative Note to SR VII: Wire Transfers.

is not further transmitted by an intermediary along the way, investigators will thus not have access to information that may help to establish terrorist links.

19. More complicated wire transfer schemes have been observed and can involve multiple wire transfers to create a complex and deliberately confusing trail of financial transactions in order to avoid detection.

20. A few common characteristics were also noted as relevant to the typologies of potential terrorist financing through wire transfers. One important characteristic is the use of false identities, "straw men" or front companies in transactions to provide clean names and thus avoid detection. Another characteristic is to channel funds through several different financial institutions so that the wire transfers appear to come from different and seemingly unrelated sources. There also seems to be some use of wire transfers through non-bank financial institutions or alternative remittance services by terrorists (informal money or value transfer systems) with the idea that avoiding mainstream financial institutions will help terrorist funding – like the proceeds of non-terrorist criminal activity – remain undetected by financial monitoring systems or investigative authorities.

Case 1: Terrorist funds collected in Country A transferred to a terrorist organisation in Country B

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

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

Case 2: A terrorist organisation uses wire transfers to move money to further its activities across borders

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

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

Case 3: Wire transfers are used as part of a terrorist fundraising campaign

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

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

21. There was agreement among the experts present at this year's meeting that, other than the generally small size of such transactions, the value of individual transfer was generally not a distinctive feature when carried out for terrorist financing purposes. Indeed, the low value of the transfers when compared with the high overall volume of such transactions is an additional factor that further complicates detection of terrorist use of the financial system. Even establishing an average size for terrorist related wire transfers was impossible, although one delegation reported observing transfers as low as the range of USD 25 to USD 500. A few experts did note, however, that wire transfers often appear to have been structured in amounts below any mandatory reporting requirements.

Case 4: Payments are structured to avoid detection

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

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

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

22. Despite these observations made for wire transfers carried out for terrorist financing purposes, the experts reaffirmed the sense that at present investigators and financial institutions still have a limited number of useful types of indicators that help to detect possible terrorist use of wire transfers. In instances when information is available on an individual cross-border wire transaction, often the only factors that may help to link the transaction to terrorism is the name of the originator or beneficiary and the originator or destination location. The size of the transaction does not seem to follow any specific patterns, although the experts believed that they are generally low either because individual instances of terrorist financing may not involve large sums of money or because there is a conscious attempt to send smaller transactions to avoid detection.

Policy Implications

23. Guidance for preventing and detecting the misuse of wire transfers systems by terrorists – and by other non-terrorism related criminals – is set forth in FATF Special Recommendation VII and in the Interpretative Note issued subsequently by the FATF. The Recommendation calls for the recording, maintaining and, in the case of cross-border transfers, transmitting of certain key elements of information on the originator of the transfer. This information, once available at the receiving end of the transfer will enable financial institutions to make initial assessments of potential terrorist / criminal connections (i.e., for purposes of suspicious transaction reporting) and ultimately to FIUs, law enforcement or other competent authorities (i.e., for the initial stages of their analytical or investigative process).

24. The inclusion and retention of meaningful originator information on a wire transfer can assist the fight against terrorist financing and money laundering in several ways. Transactions that contain

full information assist beneficiary financial institutions to identify potentially suspicious transactions. These would require extra diligence and potential onward reporting to an FIU. When reports on unusual or suspicious wire transfers are received by an FIU, those that contain complete information can be more thoroughly researched and analysed. Finally, ensuring that originator information is readily available assists the appropriate law enforcement authorities to detect, investigate and prosecute terrorists or other criminals.

25. While it was not the purpose of the workshop to look at the overall effectiveness or appropriateness of measures called for in SR VII, the general view of participants in the exercise was in support of the measures. Having "complete and meaningful" information on the originator of a wire transfer message available to financial institutions and competent authorities was deemed as critical to being able to detect or prevent terrorist and criminal use of the wire transfers.

26. The Interpretative Note to SR VII issued in February 2003 provisionally allows for the existence of *de minimis* thresholds of USD 3,000 with regard to the measures called for in the Recommendation. Thus, although countries must still require the collection and retention of originator information on wire transfers valued below this amount, the transmission of this information with the wire is not required. The experts discussed the issue of having a threshold in connection with the wire transfer measures in SR VII. The majority of experts indicated that wire transfer transactions that are potentially related to terrorism would generally involve small amounts. The consensus of the experts then was that the existence of a threshold for SR VII requirements – from an operational perspective – could hinder the detection of what might be relevant transactions. It was also noted that the lack of a threshold could also serve as a deterrent to the use of wire transfers by terrorists or criminals by making the risk of detection greater.

27. The experts also acknowledged, however, that in the absence of other specific indicators, the lack of a threshold could lead to an excessive number of transactions being reported to the FIU. Reports on individual transactions would perhaps have less value as means of detecting terrorist financing, although they would still be important in helping to build a picture of financial structures supporting terrorism when detected through other channels (for example, through intelligence reports or investigations conducted by other agencies). As indicated above, the most important elements in detecting terrorist-related wire transfers at present are the names of the parties involved and the geographical source or destination of the transaction. The experts agreed, therefore, that more work needs to be done to develop clearer indicators of terrorist use of wire transfers. These indicators could assist financial institutions in identifying the transactions that may require increased scrutiny and ultimately be reported to competent authorities as suspicious or unusual.

28. A potential solution for finding additional indicators would be to encourage the development of information technology systems that could look for objective indicators within wire transfers. One delegation proposed using a system that identifies such indicators based on key words occurring in the wire transfer messages. Establishing a score based on differing values assigned to the key words permits the system to select a smaller pool of transactions that may require further analysis.

II: NON-PROFIT ORGANISATIONS AND LINKS TO TERRORIST FINANCING

29. The FATF examined the role of non-profit organisations (NPOs) as part of its last typologies exercise (2002-2003). At that time, it was able to make some preliminary findings on the nature of the risk to the sector. In order to expand on this work, NPOs and potential for misuse for terrorist financing purposes was selected once again and became the second workshop topic for this year's exercise. As indicated in the introduction, all three workshops had additional preparation before the experts meeting. The preparation for the NPO workshop, however, was the most extensive of the three workshops, consisting of several small meetings of experts and numerous exchanges of analyses and position papers. For this reason, the NPO workshop was able to obtain a greater degree of detail in its findings which are then reflected in this report.

30. While some countries have relatively extensive experience with terrorism financing through NPOs, other countries clearly have a more limited experience. Only some of the material provided as part of this year's exercise described cases of *proven* terrorist financing. Much of the material therefore related to *suspected* or *possible* terrorist financing — many cases involved investigations that were still ongoing — while a few of the cases dealt with other possible forms of misuse of NPOs.

31. Most countries share the concern over the difficulties in detecting terrorist financing through misuse of NPOs. It is generally acknowledged that such organisations play a crucial social and financial support role in all societies, and obviously this role is not called into question. Nevertheless, the sheer volume of funds and other assets held by the NPO sector means that the diversion of even a very small percentage of these funds to support terrorism would constitute a grave problem. Therefore, the limited knowledge about the extent to which terrorists may be exploiting the sector should be considered a matter of serious concern for the whole international community.

32. NPOs possess many characteristics that are particularly vulnerable to misuse for terrorist financing. They enjoy the public trust, have access to considerable sources of funds, and are often cash-intensive. Furthermore, some of these organisations have a global presence that provides a framework for national and international operations and financial transactions, often within or near those areas that are most exposed to terrorist activity. Finally, depending on the country and legal form of the NPO, they are often subject to little or no regulation (for example, registration, record keeping, reporting and monitoring) or have few obstacles to their creation (for example, there may be no skills or starting capital required, no background checks necessary for employees, etc.).

Typologies

33. The case examples presented during this year's typologies exercise appeared to show that NPOs can be misused in a variety of ways and for different purposes within the framework of terrorism financing. First of all, NPOs can be used by terrorists and terrorist organisations to raise funds, as was the case for many of the larger NPOs that had their assets frozen on the basis of the UN Security Council Resolution 1373 (2001). Often – but not always – these organisations have applied for and received a formal charitable or tax exempt status. Moreover, some of these organisations were reported to have used rather aggressive fund raising techniques, sometimes seeking donations from the public at large, and in other instances focusing on certain target groups, particularly within specific ethnic or religious communities.

34. A number of the experts noted the importance of *informal cash collection* in many ethnic or religious communities and the difficulties in accurately monitoring those funds. Although it is most likely that the vast majority of these funds are raised and used for entirely legitimate charitable purposes, the obvious potential for abuse is nevertheless problematic. The existence or pretence of cash collections can also facilitate the integration of the proceeds of criminal activities carried out by terrorist groups into the "legal financial system". These funds are then represented as legitimate charitable cash collections for an NPO, and the process is thus a form of money laundering for terrorist purposes.

Case 5: Raising of funds through an NPO

A registered charity, ostensibly involved in child welfare, used video tapes depicting religious "freedom fighters" in action in various countries, together with graphic images of atrocities perpetrated against members of that religion. The tapes contained an appeal to send donations to a post office box number to help in the "struggle". These tapes were apparently widely distributed around religious establishments throughout the region. The same post office box number was associated with a further appeal in magazines which published articles by well known extremists.

35. NPOs can also be used by terrorists *to move funds*. In this case, terrorists exploit the fact that financial transactions which effectively transfer funds from one geographic location to another — often across national borders — are regarded as the normal business of certain types of foundations and charities. In some instances, the legal form and ostensible purpose of the NPO seem to have been chosen carefully in order to avoid regulation and monitoring (for example, cultural associations established in some countries by indigenous ethnic communities). A few apparently related case examples were cited by several delegations whereby networks of related foundations in different countries are established within a particular ethnic community and then seem to function as a framework for illegal alternative money remittances. Although it is not clear whether any of these schemes are directly related to terrorist financing, the structure of the networks is interesting because of its unusual characteristics and potential for abuse. The examples also show that there can be little to distinguish between transfers within or among NPOs and the provision of illegal money remittance services. These "alternative money remitters" make use of NPO bank accounts to collect cash deposits and settle the accounts with their overseas contacts. In some cases, these transactions were considered suspicious by the competent authorities because of the incongruity between the amounts handled and the modest living conditions of the particular community that provides financial support to the NPO in question.

Case 6: An NPO is used to transfer money to suspected terrorists

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

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

Case 7: NPOs used to make illegal transfers

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

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

36. Finally, NPOs can also be used to *provide direct logistical support* to terrorists or *serve as a cover for their operations*. This type of terrorist misuse is particularly evident among those NPOs that have several branches operating in multiple jurisdictions.

Case 8: Senior members of an NPO use the organisation to fund terrorism

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

Financial and business records were seized from the NPO's head office and the homes of the NPO's chief executive officer and a member of its board of directors. On the same date, Country X issued an order blocking the NPO's assets and records pending further investigation. Eleven months later, Country X submitted the NPO to the UN for designation under relevant UN Security Council resolutions for its support of a terrorist organisation.

Country X convicted the chief executive officer of the NPO for fraud and organised crime related offences for diverting more than USD 315,000 of charitable donations to terrorist organisations. Prior to these actions, there is evidence that the NPO had provided both direct and indirect financial support terrorist organisations.

Categories of misuse

37. An important conclusion from this year's work on NPOs is that various categories of these organisations have different sets of risk profiles and thus vary in the types of unusual characteristics that may be detected and used in identifying terrorist financing. It is important, for example, to distinguish between NPOs that officially register as charities and then use their status to tap into a broader base of funding and those NPOs that perform a less visible function, sometimes avoiding registration or tax exemption altogether. Often these unregistered NPOs obtain their funds from or provide services for certain ethnic communities. Such NPOs may be more commonly known as cultural associations or associations or foundations with community-related activities rather than as charities.

38. A distinction can also be made between NPOs that operate internationally and those that have a local function. There is a common misperception that NPOs can only be misused in an international context by raising funds in donor countries and then sending these funds abroad to terrorist groups in third countries. Although internationally active NPOs may be more vulnerable to misuse, terrorist financing may also occur within NPOs that operate exclusively within national boundaries. Countries that have an internal terrorist problem clearly have experience with NPOs operating within their borders that have been misused for the financing of local terrorist groups. A related misconception is that the misuse of NPOs by terrorists is exclusively related to religious extremism.

39. Another distinction that can be made relates to the differing degrees of complicity between an NPO and its donors. While in most of the relevant cases considered by the experts this year involved corrupt or complicit management of the NPO as a contributing if not primary reason for the link with terrorist financing, there are also reported examples of largely innocent NPOs that were exploited by a few infiltrators who were able to siphon off or divert the funds of the organisation. Moreover, an innocent NPO could also be the victim of an unrelated recipient organisation or related branch office.

There are even cases of bogus fund raising, where the name of existing and unwitting NPO was used as a cover for illegal fund-raising.

Detecting terrorist financing in the NPO sector

40. Given the typologies discussed above, the experts came to the conclusion that the method with the best chance of success for detecting possible terrorist financing links to NPOs is through intelligence or police work, which builds on links with other NPOs (operational, financial or through common management and personnel) or though connections to individuals that are already suspected of terrorist or terrorist financing activities. In some cases, the directors or managers of the NPO may already have a history of extremism or even a criminal or terrorism-related record. In other cases, links may be established with well-known terrorist organisations or with other NPOs that are already on the various lists of designated persons or entities maintained by the United Nations or individual countries. Public concerns and tips about the possible involvement of NPOs in questionable activities can also play a role in detecting possible misuse.

41. The reporting of suspicious unusual transactions by financial institutions and the subsequent analysis by FIUs or law enforcement also play an important role in bringing certain cases of suspected terrorist abuse of NPOs to the surface. In some countries, suspicious transaction reports related to unusual NPO-activity have actually led to the initiation of an investigation, while in other cases the reporting system and FIU-analysis have contributed to the development of further leads in ongoing investigations.

42. The monitoring activities of supervisory or tax authorities responsible for NPO oversight do not appear to have identified any initial leads into terrorist financing cases within the charitable sector. However, these authorities have sometimes played an important role in developing relevant leads by being able to ask further questions or inspect entities and/or share information with law enforcement agencies.

43. The experts agreed that each of these detection mechanisms had a complimentary function that could be pursued or enhanced collectively. This diversity of possible detection mechanisms and information sources regarding potential terrorist abuse of charities underscores the importance of constructing effective information-sharing arrangements both within and among government authorities.

Warning indicators

44. Besides the links to suspected terrorists, terrorist organisations or other suspect NPOs, the experts also identified a number of individual unusual characteristics or "red flags" in the case examples considered during this year's typologies exercise. Some of these unusual characteristics could be particularly helpful for financial institutions; others may be more useful for supervisory or investigative authorities.

Specific financial characteristics:

- Incongruities between apparent sources and amount of funds raised or moved such as situations in which large amounts of funds are apparently raised within communities that have a very modest standard of living.

- A mismatch between the pattern and size of financial transactions on the one hand and the stated purpose and activity of the NPO on the other, for example (as mentioned above) a cultural association that after ten years of existence opens a bank account for handling the proceeds of a music festival and deposits a disproportionately large amount of money into the account.

- A sudden increase in the frequency and amounts of financial transactions for the account of an NPO or the inverse, that is, the NPO appears to hold funds in its account for a very long period.

- Large and unexplained cash transactions by NPOs.

- The absence of contributions from donors located within the country of origin of the NPO.

Other characteristics:

- The existence of foreign directors, particularly in combination with large outgoing transactions to the country of origin of such directors and especially if destination is a high-risk jurisdiction.

- The existence of a large number of NPOs with unexplained links: for example, several NPOs transfer money to each other or share the same address, same managers or personnel; or a large number of NPOs are related to the same community and use the services of the same gatekeeper.

- NPOs with little substance, that is, in relation to their stated purpose and financial flows, or else they appear to have little or no staff, suitable offices or telephone number.

- Operations in or transactions to or from high-risk jurisdictions could of course also be considered as a reason for higher scrutiny by financial institutions. It could also serve as a criterion for initiating increased attention by supervisory or other competent authorities.

Policy implications

Different oversight systems and approaches

45. The consensus among those experts involved both in this year's typologies exercise and specifically in the NPO workshop was that additional measures will likely need to be developed to reduce the vulnerabilities of NPO to misuse for terrorist financing purposes. The extent and the nature of such measures remain to be defined, however. In part, the lack of clear direction in this area reflects the fact that there are great differences among countries in how they oversee and ensure transparency within the NPO sector. Some countries, for example, have a long-standing tradition of active government oversight of NPOs, while other countries put more emphasis on criminal investigation and detailed record-keeping requirements. Still other countries have implemented far-reaching regulatory systems that include detailed record keeping and reporting requirements, external auditors, licensing, the mandatory use of authorised bank accounts, permits for international transactions, and detailed customer due diligence requirements for banks (with regard to NPOs).

46. The differences in approach among countries appear to be mostly related to different philosophies with regard to the role of government in the regulation of charities and other types of NPOs. Some countries believe that the protection of donors is a legitimate reason for comprehensive government regulation and supervision of NPOs. Others believe that protection of donors is primarily the responsibility of those who contribute to NPOs, thus it is private watchdog organisations, etc., which are responsible for this oversight.

47. Many countries have some kind of regulation and oversight of those NPOs that have been granted a full or partial tax-exempt status by fiscal authorities. In certain countries, these authorities may even play an important and active role in the oversight of such organisations. For example, the fiscal authorities may require detailed annual reports from each registered NPO and then make this information publicly available upon request. In other countries, government regulation and oversight is mainly geared towards protecting the integrity of certain types of legal entities, which have a specific license to handle large amounts of charitable funds.

48. Finally, there is of course another reason to increase regulatory oversight of the NPO sector, namely to prevent criminal abuse, not only for terrorism financing, but also for money laundering and fraud. No matter which approach is taken, most countries still appear to have significant loopholes in their systems. The experts identified a number of important constraints that might prevent jurisdictions from effectively reducing the threat posed by terrorist financing or other criminal misuse of the NPO sector.

49. Most countries can only dedicate a limited part of its resources to the regulation and oversight of the NPO sector, which in some cases consists of hundreds of thousands of organisations that handle a significant percentage of the GDP of a country. This observation is particularly true for many of the recipient or developing countries, where NPOs of all sizes, often community-based, play a particularly crucial role in the economy. Sometimes the NPO-sector in those countries has a larger economic weight and importance than the public sector.

50. In most countries, a large percentage (up to 90%) of the total number of NPOs consists of very small organisations. For these smaller NPOs, it can be difficult to carry a substantial administrative burden that would be required for complying with detailed government regulation. Even for larger organisations, there are limits to what can be considered a reasonable compliance burden, since the resources of NPOs are by their very nature scarce in relation to the often essential services they provide. Furthermore, some countries have certain legal or even constitutional provisions that prevent or limit the imposition of regulatory requirements on certain categories of NPOs. Examples of such provisions are the freedom of association or the special status of religion-based organisations.

Conclusions and issues for follow up

51. There was a consensus among the experts of this year's typologies exercise that, whatever approach is taken, government regulation or oversight should have a risk-based character. Any oversight regime (whether a genuine regulator or tax authorities) should have a targeted function and focus on areas of high risk. An argument was made by some experts that an oversight function may be more useful in developing a terrorist financing lead in the early stages of investigation when there is not yet sufficient ground for a criminal investigation, rather than in generating independent leads. Others believed that government oversight could also have a clear preventative and lead-generating function by requiring enhanced scrutiny on certain high-risk categories of NPOs. In any event, it was recognised that having the authority and means to follow up on the suspicious or unusual characteristics of an NPO before there is sufficient grounds for initiating a criminal investigation is perhaps one of the most crucial elements of an effective system to combat misuse of the NPO sector.

52. Regardless of the approach taken to oversee of NPOs, many countries may nevertheless continues to have certain exceptions or loopholes in their systems that limit any reduction in the vulnerability of the sector as a whole. For example, some countries may be unable to monitor NPOs that do not register for tax-exempt status, religious organisations or NPOs established in certain other unregulated legal forms. There is thus a need to examine how vulnerable these parts of the NPO sector are to terrorist financing or other forms of misuse and then to identify alternative solutions to guarantee transparency and access, when necessary, to competent authorities. A solution mentioned by one country was to require NPOs to register with fiscal authorities in order to open a bank account.

53. In order to generate and develop leads, the experts considered it important to further develop or enhance mechanisms and gateways for sharing information both nationally and internationally. To facilitate co-operation on the national level, there was considerable support for the idea of creating "national task forces" of law enforcement agencies, intelligence and security services, FIU personnel, NPO supervisors and tax authorities. Such task forces could: (i) examine and assess the risk of terrorist financing in the NPO sector; (ii) recommend appropriate development or enhancement of an effective yet reasonable oversight mechanism to combat this risk, and (iii) share information on potential or suspected terrorist financing activity occurring in the sector.

54. For international information exchange and co-ordination, the experts emphasised the importance of proactive and rapid information exchange between counterpart and non-counterpart agencies (that is, not only between FIUs, for example, but also between FIUs and regulatory or law enforcement agencies). The type of information exchange would be as a complement to more formal exchanges of information, in particular if there are strong indications of internationally active groups and possible links with specific NPOs overseas. International organisations that can compare different national databases could also play a very useful role.

55. Particular attention should also be paid to removing the obstacles for tracing and verifying the use of NPO resources in third countries (overseas operations or overseas connections). This is especially problematic in distressed or conflict areas. To address this problem, a number of ideas were discussed, including: (i) the need for closer co-operation between the authorities of donor and recipient countries; (ii) the possibility of co-ordinating and sharing information resulting from occasional field audits overseas; (iii) the possibility of channelling funds through explicitly authorised and monitored local organisations; (iv) the development of a template for reliable procedures for international transactions and operations (examining the procedures of the larger and more established NPOs in each donor jurisdiction and in each recipient jurisdiction); (v) the possibility of reversing the burden of proof in certain instances (NPOs in donor countries proving that their overseas operations and transactions, also through local NPOs, are conducted in accordance with their stated purpose and by-laws), and (vi) requiring NPOs to receive licenses associated with enhanced due diligence requirements before authorising operations in certain high risk conflict or terrorist areas or jurisdictions. While none of these ideas was intended to relieve the recipient jurisdiction from all responsibility associated with overseeing the NPO sector, each proposal offers a means of enhancing protection of the NPO sector by imposing additional obligations on the donor jurisdiction or NPO. This could also help to provide sufficient protection against misuse of resources in geographical areas where there is relatively little government control particularly in conflict areas.

56. Further work needs to be done in order to make optimal use of the system for reporting suspicious or unusual transactions as a means of detecting possible misuse of NPOs. Further work also needs to be done on the red flags as well as on best practices for customer due diligence in relation to NPOs. Finally, it is important that countries engage in discussions with their NPO sector to ensure mutual understanding and co-operation in the fight against terrorism financing. It is also essential that countries make optimal use of the available knowledge and expertise in the NPO sector to determine which measures and requirements are feasible and effective and which best practices can be identified.

III: MONEY LAUNDERING VULNERABILITIES IN THE INSURANCE SECTOR

57. The worldwide insurance industry, according to some sources, generates premiums in the range of USD 2.4 to 2.6 trillion[3]. The industry provides risk transfer, savings and investment products to a variety of consumers, from individuals to multi-national corporations and governments. The insurance industry is moreover diverse; three major areas of the industry (according to the types of insurance product) include general insurance, life insurance and re-insurance. These products, like any other financial service, are exposed to a threat of money laundering, and previous FATF typologies exercises – in particular, last year's – have identified cases in which certain insurance products have been used to launder money. For this reason, the FATF selected insurance as the topic for the third workshop in this year's exercise.

58. Financial institutions view payments originating from insurance companies as commonplace. The money is assumed to be clean and the payments do not attract attention. If money launderers can place funds into an insurance policy, then they will have made significant steps in layering and integrating the funds into the international financial system.

59. The experts viewed the insurance sector as potentially vulnerable to money laundering because of the size of the industry, the easy availability and diversity of its products and the structure of its business. In regard to this last point, it is important to note that insurance is, in some jurisdictions, often a cross-border business and more frequently than not involves the distribution of its products through brokers or other intermediaries who are not necessarily affiliated with or under the control or supervision of the company that issues the product. Moreover, because the beneficiary of an insurance product is often different from the policyholder, it is sometimes difficult to determine when and for whom it is necessary to perform customer due diligence (for the policyholder only or also for the beneficiary?).

60. In order to lessen the inherent risks to the insurance industry, many jurisdictions require certain parts of the industry to be subject to formal anti-money laundering requirements, such as customer due diligence and the obligation to report suspicious transactions. There are, in addition, international anti-money laundering norms proposed by the insurance industry itself and issued through the International Association of Insurance Supervisors (IAIS)[4]. The IAIS anti-money laundering guidance paper for insurance entities identifies the main principles and procedures relevant to the industry, including compliance with know-your-customer (KYC) requirements and training programmes for staff.

61. This year's typologies exercise examined the risks, trends and vulnerabilities of insurance to money laundering and assessed the nature and size of any money laundering problem with a view to identifying which categories of insurance are most at risk of money laundering.

Typologies

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

[3] OECD (2003), *Insurance Statistics Yearbook 1994 - 2001*, p. 2; and "Sigma Insurance Research Paper 8", *World Insurance in 2002*, p. 26.
[4] For further information on the IAIS: www.iaisweb.org.

Case 9: An Insurance policy used to launder money

A money launderer purchased marine property and casualty insurance for a phantom ocean-going vessel. He paid large premiums on the policy and suborned the intermediaries so that regular claims were made and paid. However, he was very careful to ensure that the claims were less than the premium payments, so that the insurer enjoyed a reasonable profit on the policy.

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

Case 10: Money laundering following insurance firm pay outs

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

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

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

63. The examples provided in this year's typologies exercise appear to further demonstrate that there are a number of potential warning signs of possible money laundering, including the potential policy holder being more interested in cancellation terms than the benefits of the policy. The use of cash and /or payment of large single premiums – indeed, the use of large volumes of cash for any payment – should be considered suspicious and as a potential attempt to place criminal funds into the financial system through insurance products.

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

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

Case 11: Money Launderers use the insurance industry to clean their funds

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

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

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

66. Frequent changes of beneficiaries, using the policy as a bearer asset, or as collateral in part of a wider money laundering scheme together with the early surrender of investment type policies, especially where to do so defies economic logic were also noted as potential money laundering problems by some member countries.[5]

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

Case 12: Organised crime launders money through life insurance policies

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

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

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

68. The experts in this year's workshop on insurance also observed that the other insurance products may be similarly vulnerable to money laundering where there is almost exclusive use of intermediaries (again brokers or agents that are not affiliated with the company that has issued the

[5] For further potential indicators of money laundering in the insurance sector see p19 and 20 of IAIS AML guidance notes for insurance supervisors and insurance entities at: http://www.iaisweb.org/02money.pdf.

insurance product). The risk may be even more acute when the relative lack of anti-money laundering requirements or other relevant regulations for this sector is factored in.

Suspicious transaction reporting and insurance

69. An important observation made by the experts in this year's typologies exercise concerns the relatively low numbers suspicious transaction reports that involve insurance. This observation appears to be true for the majority of those participants in the workshop despite the fact that the insurance sector has been subject to suspicious transaction reporting for a number of years now in many countries. Furthermore, the number of reports does not necessarily correspond to the relative size of the industry in comparison to the financial sector as a whole. Indeed, certain jurisdictions with substantial insurance industries have very low numbers of insurance-related suspicious transaction reports, despite rigorous reporting requirements.

70. The experts considered whether relatively low numbers of suspicious transaction reports and law enforcement cases involving insurance-related money laundering indicate that the insurance sector was not being significantly used by money launderers or whether cases of money laundering are not being detected. It was the view of some of the experts that, given the size of the insurance industry, its vulnerabilities would be too great for money launderers to ignore. Some, however, believed that the high level of supervision in their countries along with the elimination of bearer policies somewhat lessened the potential risk. That said, it has been the experience in other parts of the financial sector that those parts of the financial system in which anti-money laundering procedures are inconsistently applied are those that are at most risk of exploitation for money laundering purposes.

Policy implications

71. The amount of actual money laundering detected within the insurance industry appears to be very low in comparison with the size of the industry. Nevertheless, the experts in this year's exercise believe that the insurance sector is still vulnerable to money laundering. It is possible that money laundering is not being detected within the insurance industry due to a combination of the inherent nature of the industry (the dependence on brokers for the distribution of its products), the fragmented and incomplete application of anti-money laundering rules and regulations and a lack of an industry-wide commitment to address this risk. As a first step, it will likely be necessary to better understand how and to what degree the various parts of the insurance sector could be used by money launderers.

72. In order to close the loophole of inadequately applied AML/CFT measures, an increased effort will likely need to be made to apply existing measures. There should be a better sharing of information on typologies relevant to the insurance sector, both within the industry and between it, law enforcement and supervisory agencies. Law enforcement and other investigative agencies could also be encouraged to identify any relevant money laundering typologies from other investigations, such as, for example, links with insurance claimant fraud.

73. The experts found that the main vulnerability to money laundering in the insurance industry is probably at the integration and layering stages of the laundering cycle. It is at this point that indicators may be less obvious, or a different type or degree of diligence is required to identify money laundering. Basic customer identification procedures may be insufficient without more comprehensive customer due diligence.

74. The nature of the money laundering risk in the insurance sector appears to be different from that which exists for the rest of the financial sector; consequently, there may be the need to develop industry-specific AML measures. The experts also concluded that further work is necessary to better understand and determine specific vulnerabilities across the whole insurance sector (not just with regard to life insurance).

IV: POLITICALLY EXPOSED PERSONS

75. The FATF examined PEPs and the risk they represent to the financial sector when it looked at the money laundering vulnerabilities of private banking in 2001. New revelations of suspected PEPs' involvement in financial crime – especially as related to corruption – occur frequently in the press. After issuing the revised Forty Recommendations in which there are enhanced measures meant specifically to target the risk posed by PEPs, the FATF decided as well to include a short examination of this subject as part of this year's typologies exercise. The issue was therefore discussed during the full meeting of experts, and some initial findings were made.

76. *Politically exposed person* or *PEP* is the term used for individuals who are or have been in the past entrusted with prominent public functions in a particular country. This category includes, for example, heads of State or government; senior politicians and government, judicial or military officials; senior executives of State-owned corporations and important political party officials. Because of the special status of PEPs – politically within their country of origin or perhaps diplomatically when they are acting abroad – there is often a certain amount of discretion afforded by financial institutions to the financial activities carried out by these persons or on their behalf. If a PEP becomes involved in some sort of criminal activity, this traditional discretion given to them for their financial activities often becomes an obstacle to detecting or investigating crimes in which they may be involved.

77. From the material presented during the experts' meeting and the written submissions made by participants in the exercise, several observations can be made. First, the sources for the funds that a PEP may try to launder are not only bribes, illegal kickbacks and other directly corruption-related proceeds but also may be embezzlement or outright theft of State assets or funds from political parties and unions, as well as tax fraud. Indeed in certain cases, a PEP may be directly implicated in other types of illegal activities such as organised crime or narcotics trafficking. PEPs that come from countries or regions where corruption is endemic, organised and systemic seem to present the greatest potential risk; however, it should be noted that corrupt or dishonest PEPs can be found in almost any country.

Case 13: An associate of a PEP launders money gained from large scale corruption

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

Prior to the capture of Mr. Z, an associate of Mr. Z, Mr. Y was arrested on a provisional arrest warrant and request for extradition from Country A. Mr. Z and his associates, including Mr. Y, generated the criminal proceeds forfeited in this case through the abuse of Mr. Z's official position as advisor to former the President of Country A. Some of the principal fraudulent schemes involved the purchase of military equipment and service contracts as well as the criminal investment of government pension funds.

Mr. Y was involved in a huge kickback scheme that removed money from both Country A's treasury and their military and police pension fund. Mr. Y and others used pension fund money and their own money to buy a majority interest in a Country C banking institution, Bank M, which in June 1999 was bought by another bank in Country A. Mr. Y was in charge of seeking investments on behalf of Bank M and identified construction and real estate projects for the bank and pension fund to finance. He also controlled the construction companies which built those projects. Mr. Y established a pattern of inflating the actual cost of the pension fund investment projects by 25 percent and billed Bank M accordingly. Projects recommended by Mr. Y were automatically approved by

[6] And an additional USD 22 million was later discovered.

the board members at the police pension fund, as several of them received kickbacks. A USD 25 million project was fraudulently inflated by USD 8 million. Similarly, Mr. Y covertly formed and controlled several front companies used to broker loans from Bank M in exchange for kickbacks from borrowers. When some loans defaulted, Mr. Y would purchase the bankrupt projects at extremely low prices for resale at a profit.

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

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

Mr. Y opened a bank account in Country C, and moved about USD 15 million through it until he was arrested. Initially, the account opening did not raise any suspicion because Country A nationals often opened bank accounts in the Country C to protect their assets from inflation. However, financial institutions holding bank and brokerage accounts owned or controlled by Mr. Y, Ms. D and others gradually noticed unusual activity in the accounts. According to bank officials, Mr. Y's financial transactions had no apparent business justifications and the origin of the funds was suspicious.

78. Another observation is that PEPs, given the often high visibility of their office both inside and outside their country, very frequently use middlemen or other intermediaries to conduct financial business on their behalf. It is not unusual therefore for close associates, friends and family of a PEP to conduct individual transactions or else hold or move assets in their own name on behalf the PEP. This use of middlemen is not necessarily an indicator by itself of illegal activity, as frequently such intermediaries are also used when the business or proceeds of the PEP are entirely legitimate. In many cases however, the use of middlemen to shelter or insulate the PEP from unwanted attention can also serve as an obstacle to customer due diligence that should be performed for every customer. A further obstacle may be involved when the person acting on behalf of the PEP or the PEP him or herself has some sort of special status such as, for example, diplomatic immunity.

Case 14: A senior government official launders embezzled public funds via members of his family.

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

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

79. Besides the use of third parties, PEPs involved in moving or concealing illegal proceeds generally do so by funnelling the funds through networks of shell companies or offshore banks in locations outside his or her country of origin that are not likely to divulge details of relevant

transactions. In other cases, their financial operations may be concealed behind various other types of opaque legal arrangements such as trusts. Again, the ability of a financial institution to conduct full customer due diligence and apply know-your-customer principles to PEPs in this instance is severely restricted.

Case 15: A senior employee of a state-owned company involved in high level corruption

An investigation into a senior government official Mr. A, an employee of state owned Company A, uncovered that he was in receipt of excessive payments into a number of accounts that he owned and operated. Mr. A was the vice president of Company A and had a yearly income of over USD 200,000. The investigation revealed Mr. A had 15 bank accounts in several different countries through which over USD 200 million had been transacted. Mr. A used the money placed in these accounts to gain political influence and to win large contracts from foreign governments on behalf of Company A.

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

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

<u>The senior politician, senior official</u>

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

<u>Wife of a PEP</u>

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

<u>Friend and associate of the PEP</u>

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

80. According to one FATF member, there are two principal ways in which to detect the illegal financial activities of a PEP. The first is when there is a change in government in the home country of the PEP, and his or her illegal activities are revealed by the successor regime. While this may the clearest available indicator, it is not completely reliable. In some instances, accusations or illegal or corrupt practices by the new government represent a "political settling of scores". The second way

that a PEP's illegal financial operations might be detected is through suspicious or unusual transactions in which persons acting on his or her behalf may be involved. When these transactions are viewed in the context of the relationship between the middleman and the PEP on whose behalf he or she may be acting, there may then be more reason to suspect an illegal source for the funds or assets involved.

81. In addition to the potential obstacles indicated above for conducting due diligence on PEPs, applying know-your-customer principles or detecting links between them (or their associates) and criminal activity, sometimes investigations into suspected illegal financial connections may be hampered by specific factors associated with PEPs. The most important of these, according to one of the participating experts, is the lack of necessary "political support", especially when the investigation appears to show connections between the foreign PEP and senior officials in the government where investigation is taking place. Obviously, the inability to obtain needed information – or to obtain it in a timely manner – from foreign counterparts also hinders the successful completion of such investigations.

Case 16: Laundering the proceeds of embezzlement

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

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

Policy implications

82. Several implications for AML/CFT measures arise from the discussion of PEPs during this year's typologies exercise. It was emphasised by more than one expert that dealing with the financial activities of a PEP in one respect is the same as dealing with those of any customer of a financial institution: proper due diligence should be conducted on both a PEP or the persons acting on his or her behalf. Similarly, know-your-customer principles should be applied without exception.

83. With regard to persons who either are or appear to be acting on behalf of someone else, either in performing financial transactions or holding assets, determination should be made as to the real or ultimate beneficiary / owner. One delegation raised issue of the difficulty once the true owner has been determined of finding out if the person is a PEP in his country of origin. It was pointed out that senior officials often change – even within an individual jurisdiction – thus someone who is a PEP now might no longer be so in the next government. Two possible solutions were indicated: one would be to create a database that would contain information on current senior government officials. While this solution might be ideal, some delegations pointed out the difficulties that maintaining such a database would entail. Another solution would be simply to maintain appropriate databases at national level and then further encourage informal co-operation (for example, among FIUs) in enquiring about possible PEPs and their financial connections.

84. The FATF experts concluded that the techniques employed by PEPs to launder illegal proceeds were very similar to those of other criminal money launderers. If solely viewed from the perspective of the financial institution, these techniques look exactly the same. It has been noted in previous typologies exercises that PEPs may use distinctive banking arrangements to assist them in creating a complex or sophisticated network of transactions to protect illicit assets they may have generated. Again, this was indicated as another important reason that financial institutions should perform all the necessary due diligence on PEPs, including their obligation to report suspected cases of money laundering.

85. Finally, while it was understood that the issue of PEPs extends by definition only to senior-level "exposed persons" and their associates, the experts believed that the issue of corruption below the senior level is also important. In the words of one delegation, the "biggest risk" to the financial system in some jurisdictions "is the underlying culture of corruption" and, in particular, the underpaid government official holding important responsibilities. The experts considered that this issue must be addressed in a systematic way with a global approach that takes into account the differing nature and degree of corruption in both developing and developed countries.

V: GATEKEEPERS AND MONEY LAUNDERING

86. As anti-money laundering measures are implemented in financial institutions, the risk of detection becomes greater for those seeking to use the banking system for laundering criminal proceeds. Increasingly, money launderers seek out the advice or services of specialised professionals to help facilitate their financial operations. This trend toward the involvement of various legal and financial experts, or gatekeepers, in money laundering schemes has been documented previously by the FATF[7] and appears to continue today. The revised FATF Forty Recommendations issued in June 2003 address this issue by calling for the expansion of preventative financial measures to legal and financial professionals that are at risk of being involved in money laundering.[8] For these reasons, the FATF decided to look once again at how the services of these professionals may be misused for money laundering purposes.

87. Solicitors, notaries, accountants and other similar professionals perform a number of important functions in helping their clients organise and manage their financial affairs. First of all, they provide advice to individuals and businesses in such matters as investment, company formation, trusts and other legal arrangements, as well as optimisation of tax situation. Additionally, legal professionals prepare and, as appropriate, file necessary paperwork for the setting up of corporate vehicles or other legal arrangements. Finally, some of these professionals may be directly involved in carrying out specific types of financial transactions (holding or paying out funds relating to the purchase or sale of real estate, for example) on behalf of their clients.

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

Case 17: Accountant and lawyers assist in a money laundering scheme

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

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

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

[7] See previous typologies reports: FATF-IX: http://www.fatf-gafi.org/pdf/TY1998_en.pdf, FATF-XI: http://www.fatf-gafi.org/pdf/TY2000_en.pdf and FATF-XII: http://www.fatf-gafi.org/pdf/TY2001_en.pdf

[8] Recommendation 12 now calls for extending certain obligations for customer due diligence and record keeping to lawyers, notaries, other independent legal professionals and accountants. Recommendation 16 extends to this category of professionals the obligation to report suspicious transactions, subject to professional secrecy or legal professional privilege.

Case 18: Legal professionals facilitate in money laundering

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

The investigations conducted in Country Y, following a report from the FIU established that the creation and implementation of this money laundering channel had been facilitated by accounting and legal professionals - gatekeepers. The gatekeepers had helped organise a number of loans and helped set up the different legal arrangements made, in particular by creating the non-trading real estate investment companies used to purchase the real estate. These professionals also took part in managing the structures set up in Country Y. The investigation is ongoing

Case 19: An accountant provides specialist financial advice to organised crime.

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

89. A number of FATF members have begun to look more closely at the role of gatekeepers in facilitating money laundering. In one jurisdiction, which has extended the obligation to report suspicious transactions to independent legal and financial professionals, it found that less than two percent of reports dealing with solicitor or notary involvement were made by the professions themselves. It was thus in the vast majority of cases the financial institutions that detected potentially suspect activity. Among these reports, nearly 40 percent were related to the opening or administering of "trust accounts". Actions considered suspicious included cash transactions into or out of the account in rapid succession, flows of funds into or out of the account involving unknown sources or from sources that appeared to have no explainable relation, and transactions in amounts that appeared incompatible with their stated economic purpose.

Case 20: A lawyer uses offshore companies and trust accounts to launder money

Mr. S headed an organisation importing narcotics into country A, from country B. A lawyer was employed by Mr. S to launder the proceeds of this operation.

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

In Country A, a distinct group of persons and companies without any apparent association to Mr. S transferred large amounts of money to Country D where it was deposited in, or transited through Mr. S's offshore companies. This same web network was found to have been used to transfer large amounts of money to a person in Country E who was later found to be responsible for drug shipments destined for Country A;

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

Case 21: A solicitor uses his client account to assist money laundering

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

90. Another FATF jurisdiction indicated that organised crime groups were further insulating themselves from detection by using one or more "corrupted" gatekeepers to channel funds through structures set up by another layer of gatekeepers. In this way, the second level of gatekeepers did not need to be as fully implicated in the scheme, and the risk to the organised crime group was further reduced by additional separation from the money laundering process. Two particular preferred methods using gatekeepers and identified by this jurisdiction were real estate transactions and the use of legal and accounting experts to build impenetrable audit trails. In the former case, land transfers or "conveyancing" is used because relatively large amounts of criminal proceeds can be efficiently laundered in a single transaction. This delegation also noted that accounting professionals involved in setting up the complex audit trail for a money laundering scheme often may not become known to investigators because they do not actually handle directly any of the relevant financial transactions.

Case 22: A trust fund is used to receive dirty money and purchase real estate

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

Policy implications

91. Many experts noted that even when the obligation already exists for gatekeepers to report suspicious transactions, the number of reports is often low. While in some jurisdictions this may be attributable to the relatively recent implementation of such rules, there are still may be perceived obstacles to full participation of gatekeepers in the anti-money laundering system. This in large part could be due to lack of awareness on the part of these professions or hesitations due to traditions of professional client secrecy. It was pointed out by one delegation, however, that gatekeepers have access to information that could be critical in understanding complex money laundering schemes, and theirs would therefore be a critical contribution in detecting such schemes. It is thus important that legal and accounting professionals involved in providing financial services or advice have the clear legal framework within which to report suspicious transactions.

92. It is also apparent that both gatekeepers and the financial institutions with which they deal should carry out the full customer due diligence procedures. Most likely the number of legal and

financial professionals knowingly involved in facilitating money laundering is rather small. However, as indicated by many of the experts in this year's typologies exercise, one of the key reasons that services or gatekeepers are sought out by criminal organisations is to offer the appearance of additional legitimacy to their financial operations.

CONCLUSION

93. As indicated at the beginning of this report, the goals of this year's typologies exercise were to examine subjects of particular relevance to the current work of the FATF and to follow up on methods or trends initially identified in earlier typologies work. Terrorist financing and the implementation of the Eight Special Recommendations remain a primary concern of the FATF, thus examination of the role of wire transfers and non-profit organisations in terrorist financing in this year's exercise was deemed essential to the FATF's overall work. This year's look at money laundering vulnerabilities of the insurance sector expands on some of the issues identified in last year's exercise. While PEPs and gatekeepers have been addressed before by previous exercises, their inclusion in this year's programme is justified by the issue of the new FATF Forty Recommendations which provide a number of measures intended to deal with the risks in these two areas.

94. A new approach was used in preparing for the exercise and examining three of this year's topics (wire transfers, non-profit organisations and the insurance sector). This approach involved additional analysis and debate of the topics prior to the experts' meeting. It also included workshops during the experts' meeting itself to promote increased focus and serve as an additional means for exchanging ideas on the issues. The reaction of the experts to this new approach was for the most part positive, and it is therefore likely that organisers will use this experience to further improve future typologies exercises.

95. With regard to wire transfers and their connection to terrorist financing, the experts concluded that this was a mechanism that is frequently used to support various types of terrorist organisations. While investigators have been able to reconstruct terrorist links through use of wire transfers after such use has been detected, the fact that many cross border transfers do not include full identifying information on the originator is a key obstacle in determining those links. Furthermore, the initial detection of terrorist use of wire transfers remains difficult at present given the generally small size of individual transactions and the general lack of other useful indicators.

96. Non-profit organisations and their role in facilitating terrorist financing continue to be a key concern of the FATF. The experts in this year's typologies exercise made progress in understanding the types of misuse of NPOs and the specific financial "red flags" that may be indicative of it. The experts also attempted to identify some of the issues concerning oversight systems for this sector and measures that might be applied to reduce the vulnerability of NPOs to exploitation by terrorists. Additional work will need to be done to further refine this understanding of the terrorist financing risks as they relate to specific parts of the NPO sector in some countries.

97. This year was the first time that the FATF has looked at the risks that are specifically associated money laundering in the insurance sector. The experts discussed whether the amount of money laundering detected in the sector seems disproportionately small when compared to the size of the sector as a whole. Moreover, there are potential vulnerabilities that appear to be inherent to the sector. However, the experts did not reach consensus on these issues. A better understanding of these vulnerabilities as they relate to specific areas or product types seems to be emerging; however, the experts agreed that more work will need to be done to ensure that all risk areas have been identified. As well, work may be necessary to develop additional indicators specifically related to these areas.

98. Previous FATF typologies exercises have looked at some of the money laundering risks associated with politically exposed persons. The discussions of presentations and material provided for this year's exercise on this subject confirms earlier observations both as to the nature of and trends associated with this risk. While certain cases show that PEPs have used middlemen or other intermediaries to avoid detection, very often it seems that a PEP's illegal financial activities would have become clear if the financial institution opening or operating the account would have performed appropriate customer due diligence. The experts drew attention to some of the difficulties in determining whether a person should be considered a PEP, and for now, the best solution seems to be reinforcing informal co-operation among counterparts on the international level.

99. Similarly, the FATF has also examined some of the risks associated with the services provided by specialised legal and financial professionals, so-called gatekeepers. Again, the work during this exercise confirmed and expanded somewhat an understanding of the specific characteristics of this sector that make it vulnerable to money laundering. Many FATF members have begun implementing measures that would bring gatekeepers under the same obligations as currently held by financial institutions with regard to customer due diligence, record keeping and suspicious transaction reporting. A number of experts stressed that some of the vulnerabilities or risks identified regarding gatekeepers – as well as for dealing with PEPs – could be lessened if AML/CFT measures are consistently and thoroughly applied.

100. Countries from throughout the world – both FATF and non-FATF members – as well as a number of international organisations participated in the FATF-XV typologies exercise. Their experts were able to bring together the diverse experiences of individual jurisdictions in confronting the challenges of money laundering and terrorist financing and then apply them to the five themes of this year's exercise. While efforts such as the FATF typologies exercise help to increase awareness of the specific topics selected for a particular exercise, they also serve as an important forum for exchanging views between experts from operational backgrounds (i.e., police, prosecutors, regulators, FIUs) and those from the policy making side of government. It is this exchange of views that is ultimately an essential element of the FATF's efforts to promote and, as necessary, further refine the Forty Recommendations and the Eight Special Recommendations on terrorist financing.