Financial Action Task Force on Money Laundering

Groupe d'Action Financière sur le Blanchiment de Capitaux

Report on Money Laundering Typologies 2000-2001

FATF-XII

1 February 2001

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

[EN]

FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING REPORT ON MONEY LAUNDERING TYPOLOGIES FOR 2000-2001

I. INTRODUCTION

1. The Financial Action Task Force on Money Laundering (FATF) held its annual meeting of experts on money laundering methods and trends on 6 to 7 December 2000. The group of experts met in Oslo, Norway, under the chairmanship of Mr. Lars Oftedal Broch, Supreme Court Judge. The group of experts included representatives from FATF members: Argentina; Australia; Austria; Belgium; Canada; Denmark; Finland; France; Germany; Greece; Hong Kong, China; Ireland; Italy; Japan; Luxembourg; Mexico; the Netherlands; Norway; Portugal; Singapore; Spain; Sweden; Switzerland; Turkey; the United Kingdom; and the United States. The FATF-style regional bodies were also represented (see below), as well as the following observer international organisations: Europol, Interpol, the International Organisation of Securities Commissions (IOSCO), the Offshore Group of Banking Supervisors (OGBS), and the World Customs Organisation (WCO).

2. This was the second year that FATF-style regional bodies were invited to send experts from their member countries to this forum. Also in attendance therefore were representatives from: the Republic of Korea and Pakistan (member countries of the Asia Pacific Group on Money Laundering); the Bahamas and Panama (member countries of the Caribbean Financial Action Task Force); Bulgaria, Latvia, Liechtenstein, Romania, Slovenia and Ukraine (member countries of the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures [PC-R-EV Committee]); and Namibia and Tanzania (members of the newly formed Eastern and Southern Africa Anti-Money Laundering Group [ESAAMLG]).

3. The FATF typologies exercise provides a venue for law enforcement and regulatory experts to identify and describe current money laundering methods and trends, emerging vulnerabilities, and potential counter-measures. The discussions at the Oslo meeting were preceded by presentations and debates on a series of major money laundering issues agreed upon beforehand by the FATF Plenary. The primary focus of this exercise, as it is each year, was on developments in and observed by FATF member jurisdictions. However, given the increased participation of countries from outside the FATF, the experts also devoted part of the meeting to hearing presentations on the trends in other regions of the world.

4. As in previous typologies exercises, delegations and invited experts submitted written material to serve as the starting point for debate and to provide supplemental information for the report. This document is the report of the FATF-XII exercise on money laundering typologies and reflects, therefore, the ideas discussed at the experts meeting and incorporates other material as submitted by each participating country or organisation. The report is divided into two parts. The first part deals with the five major issues examined by the experts group. These include: on-line banking and Internet casinos; trusts, other non-corporate vehicles and money laundering; lawyers / notaries, accountants and other professionals; the role of cash vs. other payment methods in money laundering schemes; and terrorist related money laundering. The second part of the report focuses first on money laundering trends as they have been observed in FATF member countries and second on trends for other regions of the world. In an effort to make this report more relevant to the reader and to illustrate better some of the issues confronting authorities responsible for combating money laundering, case examples have been provided throughout the text.

II. MAJOR MONEY LAUNDERING ISSUES

(i) On-Line Banking[1] and Internet Casinos

a. General

5. When the FATF examined on-line banking during last year's typologies exercise, most experts, along with their national delegations, expressed serious concern about the vulnerabilities that the Internet might offer for money laundering. Concrete indicators for such use by criminals were not available at that time, however, and practical countermeasures had not been fully developed. For these reasons, the FATF decided to address the on-line banking issue again during the FATF-XII typologies exercise and to expand consideration of web-based laundering to other areas including gambling through the Internet.

b. Use of web-based financial services for money laundering

6. During the past year, the number of financial institutions offering on-line banking facilities has continued to grow. Virtually all FATF members now report a presence, if not an increased one, of financial services[2] offered in their jurisdictions through the Internet. The range of services available also appears to be growing – along with the acceptance and usage of electronic payment systems by the general public. However, these trends vary from one jurisdiction to another. In Hong Kong, China, for example, cash payments are the norm, and, although banks offer on-line banking services, the public currently favours the use of automated teller machines (ATMs) or direct contact with the financial institutions. In Finland on the other hand, almost half of the population has access to Internet, and some 85% of retail payment orders are transmitted to banks electronically.

7. The discussions on on-line banking during the FATF-XII typologies exercise reinforced many of the concerns raised during last year's exercise. Transactions performed by access to financial services through the Internet do not appear to present specific risks for money laundering in and of themselves. Rather, it is three characteristics of the Internet that together tend to aggravate certain "conventional" money laundering risks: (1) the ease of access through the Internet, (2) the depersonalisation of contact between the customer and the institution, and (3) the rapidity of electronic transactions. Although these factors could be considered as contributing positively to the level of efficiency and the reduction of costs of financial services, they also make customer identification and routine monitoring of accounts and transactions by financial institutions more difficult.

c. Implications for customer identification

8. A potential risk exists at any first stage of the contact between a new customer and a financial institution. The financial institution must deal with certain difficulties which are essentially the same regardless of the type of account. It must verify the identity of a natural person, who may, for example, present false or forged documentation. It must establish adequate identification of legal entities when determination cannot be made of the legal existence or nature of the business. It must also verify the signature authority for any account that is opened when it is not clear whether the customer is acting on his own behalf. In the case of Internet banking, the difficulties for the financial institution are increased if the procedures for opening such an account are permitted to take place without face to face contact or without a link to an already existing traditional account.

---

1 "On-line banking", for the purposes of this typologies exercise, focuses primarily on Internet banking, that is, banking in which the account holder accesses his or her account by means of the Internet.

2 The range of possible financial services available through the Internet includes direct payments, electronic funds transfers, issue of cheques, purchase of securities and opening/closing of accounts.

d. Implications for Know-Your Customer policies

9. Once the initial identification of the customer has been accomplished, it is usually assumed by the financial institution that it is the identified customer who continues to perform transactions on the account. This assumption is probably a valid one for traditional bank accounts. However, if an account is accessed through the Internet, there is no human intervention that might help to detect suspicious or unusual activity, such as instances in which individuals other than the account holder perform transactions on the account. Information on access to the account from other geographic locations – another possible indicator of unusual activity – would also not necessarily be detectable.[3] Furthermore, account managers may be responsible for too many accounts and therefore less able to monitor activities of individual account holders – even if ultimately equipped with monitoring software.

e. Jurisdictional issues

10. Determining jurisdiction for the licensing and supervision of financial services offered through the Internet remains a concern for the FATF. Financial regulatory agencies may not be able to ensure that financial services available through the Internet within their national jurisdictions (but from servers outside the jurisdiction) follow adequate anti-money laundering procedures. From the investigative perspective, jurisdictional issues arise in determining where an on-line transaction has taken place in order to know where investigative authorities should go to seek documentary evidence of transactions linked to money laundering activity.[4]

11. Despite the very real concern expressed by the FATF experts and delegations as to potential vulnerabilities to money laundering mentioned above, the experts were not yet able to provide case examples of money laundering through on-line banking. The lack of such evidence, however, was not considered a sign that laundering is not taking place through on-line connections. Rather, some experts believe that adequate means of detecting this type of laundering activity have not yet been fully developed. Moreover, since last year, a few FATF jurisdictions have become aware of laundering activities that have used other types of web-based activities as a cover (see the discussion below).

f. Other ways of using the Internet to facilitate money laundering

12. During last year's typologies meeting, the experts were not able to put forward any concrete examples of money laundering through the Internet; however, they were able to describe numerous instances in which various types of fraud had be committed by this means. For the FATF-XII meeting, some jurisdictions were able to present cases in which laundering is believed to have taken place using virtually the same methods found in some of the previously examined fraud cases. In both types of cases, it appears that the perpetrators take advantage of the near anonymity that can sometimes be achieved through Internet communication on the Internet, as well as the difficulty in following the path of communication links from one Internet server to another.

---

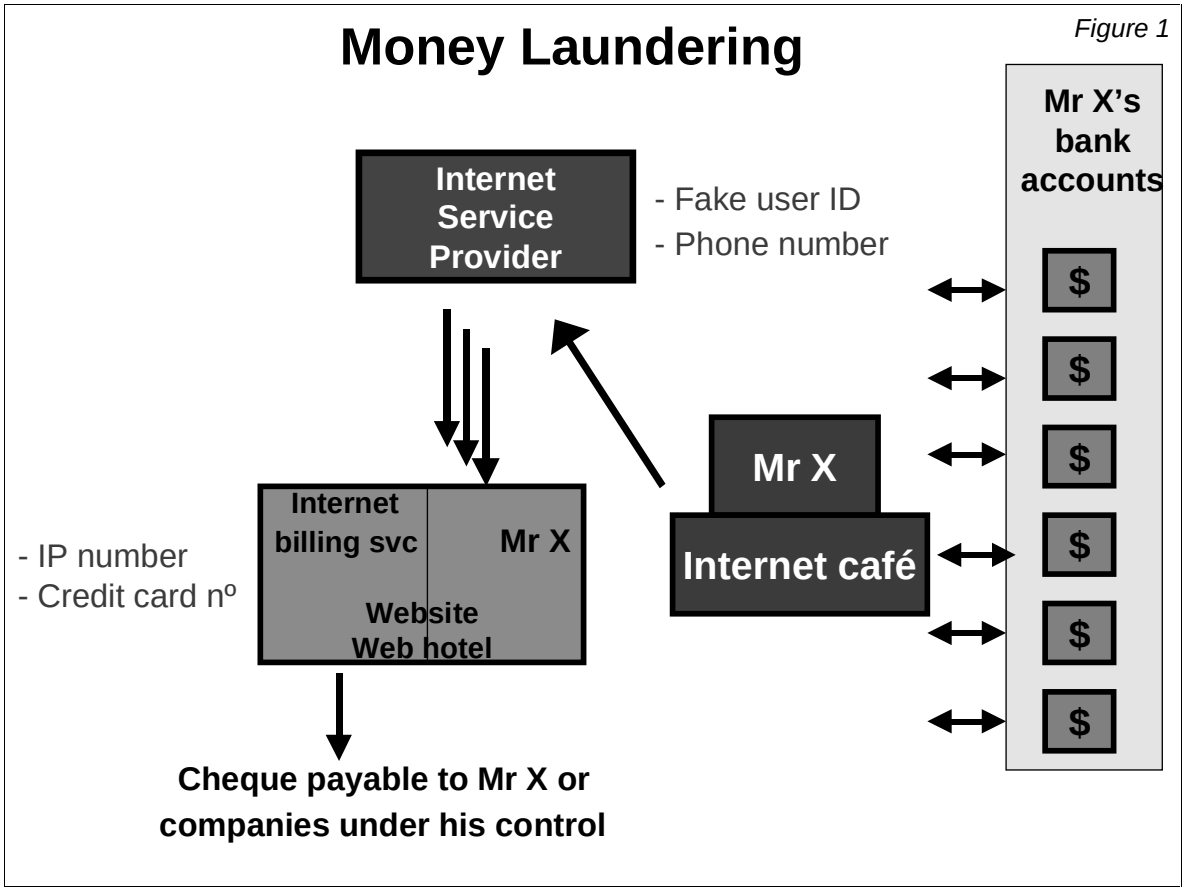
3 See *FATF-XI Report on Money Laundering Typologies, 1999-2000*, for further discussion of this issue.

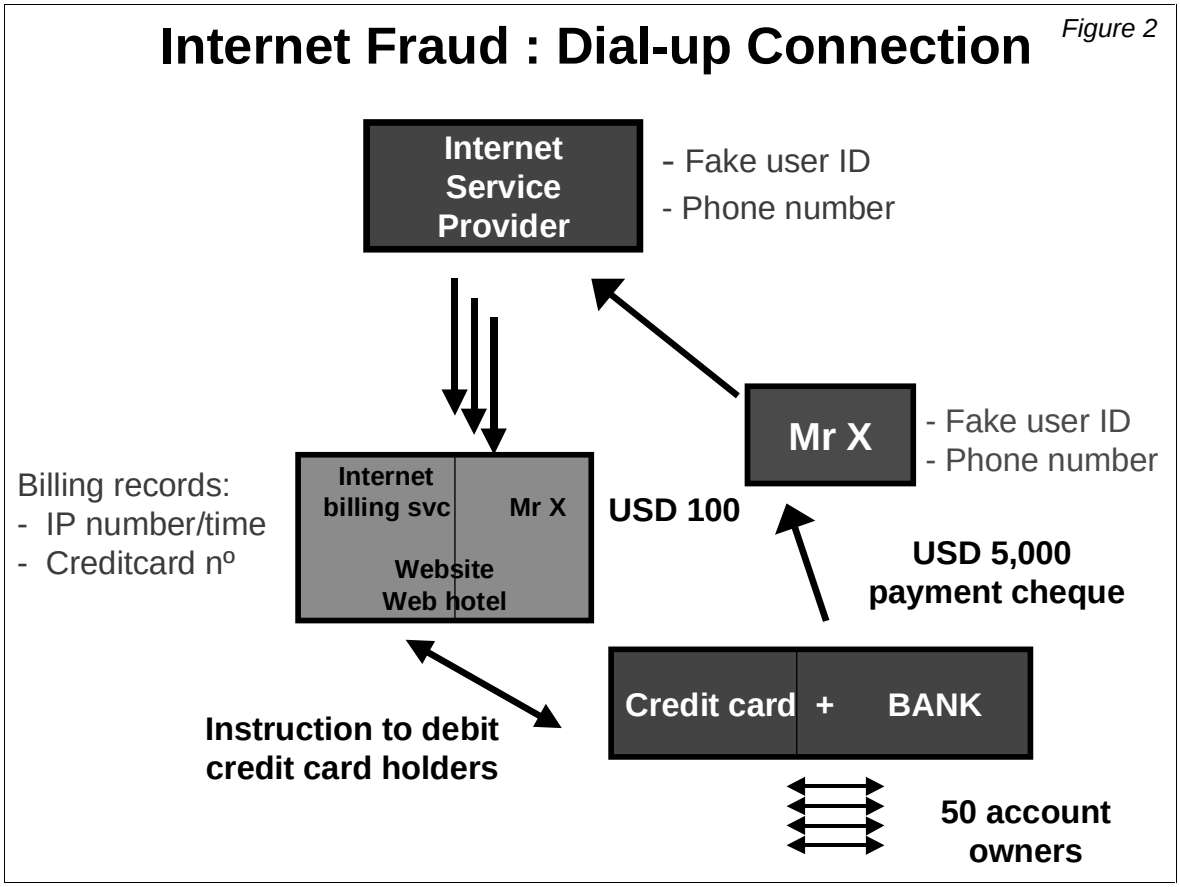
4 In this regard, a recent joint Bank of France and French Banking Commission report proposes using the logic that the Internet serves as a vehicle for accessing an account (in a similar way to accessing a bank account through the telephone). Therefore, a transaction should be considered to have taken place in the computer that includes the financial service provider's information and management system. "If the server hosting the provider's web site is not in the same location as its management system where the accounts are held, then the latter could be considered as the relevant location." – Bank of France and Banking Commission, *Internet : The Prudential Consequences*, 5 July 2000, p. 17.

g. Fraud or laundering?

13. One method of money laundering through the Internet would be to establish a company offering services payable through the Internet. The launderer then "uses" those services and charges for them using credit or debit cards tied to accounts under his control (located perhaps in an offshore area) which contain criminal proceeds. The launderer's company then invoices the credit card company which, in turn, forwards the payment for the service rendered. The launderer's company may then justify these income payments for a service rendered (See Figure 1). In this example, the launderer actually controls only the invoiced accounts and the company offering services through the Internet. The credit card company, the Internet service provider, the Internet invoicing service, and even the bank from which the illegal proceeds begin this process would likely have no reason to believe there was anything suspicious about the activity, since they each only see one part of it. Indeed, this method is virtually the same as used in many fraud cases with the difference being that, in the latter, the bank accounts billed belong to innocent third parties rather than the perpetrator of the scheme (See Figure 2).

Figure 1





14. The problem for the investigator in dealing with such schemes is being able to follow the links between the various parts of the scheme. The launderer can easily use fictitious identities in setting up his presence on the web. If he takes advantage of the easy access to Internet services in other geographical locations so as to ensure additional distance between him and his activities, he can be sure that the lack of uniformity in maintaining on-line communication records by service providers will also work to ensure his anonymity. The fact that the various components of the scheme only see part of the picture means that it will be very difficult to determine if illegal activity is taking place without first obtaining a picture of the whole operation. In short, the criminal using the Internet takes advantage of certain inherent aspects of the system to ensure that the whole picture is not visible by the investigator. To understand this better, it is perhaps worthwhile to provide some explanation of how Internet communication is organised.

h. The Internet communication trail

15. All information conveyed through the Internet[5] passes through a series of computer servers. Each connection from a particular server should leave traces (i.e., a record of its IP number, date and time of connection, etc.) on those servers with which it communicates. This information is only available, however, if the receiving servers at each step have been set up to create "log files". If the log files exist at each step and the user sending the information has a fixed IP address, it is relatively straightforward to trace back from the addressee to the originator. In instances where the user is operating using dial-up access, his or her identity can be discovered through the log files of the ISP. However, if the log files are not maintained at any step of the way, or dial-up user (or subscriber) information is considered to be protected information, then it may be more difficult to determine the ultimate link between an illegal activity and a specific individual.

i. Internet gambling

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

Example 1: A "virtual" casino is used to launder funds generated by an organised crime group

The national police force of a European country (Country A) is currently investigating a virtual casino on the Internet discovered by an analysis unit of the national customs service; simultaneously, the country's financial intelligence unit (FIU) received a suspicious transaction report from a bank which noticed significant movements of funds associated with the virtual casino. Preliminary investigation showed that the operation was run by a company in Country A. The rules of play for the virtual casino specify that it is possible to make wagers directly simply by providing credit card information.

The website of the virtual casino was located on a server maintained in the Caribbean region. To gain access to the gambling services of the site, the user had to download a relay application from an Internet service provider in Country A. The site also belonged to a firm from Country A whose headquarters is located in the southern part of the country. The person in charge of the company made an investment in another company situated in a different Caribbean jurisdiction. Through this second company, he the company bought an Internet domain name "GAME.COM". He then transferred the ownership of the name to yet another company based in the Far East.

The customs service and the FIU of Country A uncovered movements of funds involving several companies and their

[5] Internet is a global "network of networks" which is used for communicating digital information. This communication takes place between servers and services in a system that relies on and thus in some ways overlays the telephone communication infrastructure. Information communicated through the Internet is converted to digital format in what are called "packets". Each packet carries information about its originator and destination, that is, the sending and receiving servers. To ensure that these information packets arrive at their intended destination, every internet server has a unique "address" or "internet protocol (IP) number". There are approximately four billion IP numbers in use world-wide. Certain of these numbers have been assigned to specific Internet users who thus have "fixed IP addresses". Despite the high number, there are simply not enough numbers for every Internet user to receive an individual address, however. IP numbers are therefore often assigned to a user on a temporary basis by his or her Internet service provider (ISP). These users have the IP number while connected to the Internet. Once they have exited the service, the IP number is assigned to the next active user. Temporarily assigned IP addresses are usually associated with dial up connections to the internet.

management. Money flows appeared in a bureau de change and a shopping centre in Country A, as well as in several companies from the Far East, the Caribbean region, and a neighbouring European country (Country B). The connections between these various firms still must be determined.

The person in charge of the bureau de change was known by the police for violations of gaming legislation; a stockholder was allegedly involved in a bank hold up. The company located in Country B was also the subject of an investigation on gambling by its own authorities. According to these authorities, the virtual casinos represent one of the methods for laundering funds derived from criminal activity in Country B.

From this information, it was possible to conduct and investigation that revealed two illegal activities within the same company. The first of these consisted of producing components (motherboards) for operating slot machines, an activity that is prohibited by Country A's law. The profits generated by this activity (sales in Country B) were estimated at USD 739,400 for 1998 as determined from documents seized in Country A; corresponding figures were not found in the accounting records of the Country B company.

The second activity, also prohibited by Country A law, was related to the planning, creation and operation of a virtual casino on an Internet website in Country A and hosted by a service provider also located within its territory.

The customs service identified the gaming activity during a short period of 56 days at the end of 1998. The investigation by the Country A national police force did not reveal a longer period of activity because of the transfer of the casino to other websites that have not been found.

During the period of activity, 23 gamblers were able to be identified. They were from Europe, North America and Africa. There were 170 connections for wagers of USD 40,300. The authorisation to play occurred after verification of the credit card. A line of credit was opened for a defined limit.

Funds credited to a company from a third European country were transferred to the Far East and then came back to Country A (bureau de change and store).

However, the flow of funds proved to be greater than that which would have been generated simply from the identified gaming operations. Indeed, funds without justification (false invoices) were regularly transferred to the account of still another Country A company amounting to USD 94,000. One transfer for USD 268,500 to the account of the bureau de change was ultimately transferred to the personal account of the manager.

Example 2: USD 178 million laundered through Internet gambling scheme

A joint investigation by the national criminal and fiscal police of Country C targeted a sports tout service (STC) providing its gambling services by means of the Internet. The STC also functioned as an Internet service provider (ISP). The STC collected, collated and analysed statistical and other information relative to sporting events, and then sold this information to subscribers who would factor it into their betting decisions. The targeted STC/ISP expanded its services to include two offshore gambling operations located in the Caribbean region, both of which accepted wagers via the Internet or toll-free telephone numbers. Agents were successful in infiltrating the targeted operation.

To launder the proceeds from their illegal Internet gambling activities, the subjects of this investigation employed the services of a lawyer. He devised an elaborate scheme in which the STC/ISP leased its services to the subjects for a specified amount. Proceeds were also laundered through a series of bank accounts in the Caribbean area and eventually funnelled back to banking institutions in Country C. Investigators estimate that approximately USD 178 million was wagered through the STC/ISP annually.

It is anticipated that subjects in this investigation will be charged with gambling, money laundering, tax evasion and other organised crime related offences.

Example 3: Using a close resemblance to mask a laundering operation

The experience of the FIU from Country D shows that the following scheme is often used by criminals operating in that country:

An individual from Country D registers a gambling company "Gamblerz.com" in Country E where the name of the company is very similar to the name of a gambling company in Country F - "Gamblers.com" which operates legally and which has

obtained a license. Thereafter, a website to promote the information on the game is set up in Country G in the name of "Gambler.com" which in turn is an abbreviation and common to both companies. Then an account is opened in Country H and thousands of people from Country J transfer their money to that account. The criminal can operate with the funds held in the said account with the help of a modem.

The Individual withdraws USD 1 million by means of a modem from his account held with the bank RECORD. The activities are continued for several months but no license is obtained. As soon as the bank starts to query about the transactions the individual who set up the operation (male) contacts the bank by telephone. Later another person (female) provides the documents requested by the bank; however, the documents do not seem to be genuine and marks of forgery can be detected.

The bank freezes the account and reports to the FIU which takes the necessary steps in preparing materials for the police. Since it is it is a problem to determine in which country the crime has been committed, Country J opens a criminal case and launches criminal investigation to protect its own nationals who appear to be victims.

j. Possible counter-measures[6]

17. The concerns expressed by FATF members regarding the money laundering risks of on-line banking, Internet gambling and other web-based activities are being addressed in various efforts to set up harmonised standards for dealing with all forms of illegal activity conducted through this medium. One such effort is the draft Council of Europe Convention on Cyber-crime. Work conducted by the Electronic Banking Group of the Basle Committee, along with some of the measures put into place by various national supervisory authorities, represent other attempts to respond to some of the concerns regarding customer identification procedures.

18. Regarding the difficulties of following Internet links between possible criminal proceeds and the individual attempting to launder them, the experts offered the following suggestions:

- Require Internet service providers (ISPs) to maintain reliable subscriber registers with appropriate identification information.
- Require ISPs to establish log files with traffic data relating Internet-protocol number to subscriber and to telephone number used in the connection.
- Require that this information be maintained for a reasonable period (6 months to a year[7]).
- Ensure that this information may be made available internationally in a timely manner when conducting criminal investigations.

(ii) Trusts, Other Non Corporate Vehicles and Money Laundering

a. General

19. For a number of years, there has been the growing perception among FATF members that trusts and other entities that do not necessarily fall under the category of legal person[8] – along with the various forms of corporate entities – often facilitate the work of the money launderer. Although not exclusive to English-speaking countries or common law systems, trusts in their modern form are often

6 See *FATF-XI Report on Money Laundering Typologies, 1999-2000*, p. 4 The relevant concerns and counter-measures proposed in the 1999-2000 report primarily deal with customer identification issues as related to Internet banking. This year's suggested actions should therefore be viewed as complementing those put forward in the FATF-XI report.

7 There is not yet agreement on exactly how much time would be sufficient. The minimum period suggested by various authorities and the industry itself ranges from six months to one year or more. Certain of the FATF experts underscored the need, however, for standardisation of this minimum period for retention of logfiles at ISPs in all jurisdictions.

8 For example, the *Anstalt* ("establishment"), *Stiftung* or *stichting* ("foundation") and certain types of limited partnerships and limited liability partnerships found in some European and Caribbean jurisdictions.

closely associated with the legal and commercial practices of those jurisdictions. In some instances, easy trust formation and the inability to obtain information on them have been identified as an important characteristic of some non-cooperative countries and territories.[9] From the perspective of the law enforcement investigator, trusts and other similar legal relationships frequently appear to be just one more mechanism for hiding the true beneficiary or owner of assets or property derived from or associated with criminal activity.

b. Nature of trust

20. The trust as a concept originally developed in Europe as a lawful and legitimate means of protecting property or assets so that they could be used for the benefit of certain individuals or purposes. It has become a very flexible legal instrument that is now often used to consolidate or administer inheritances, assist in the financial management of companies, establish mutual investment funds, manage charitable works, sponsor cultural events or institutions. In some cases, it is used to protect assets from legitimate creditors although legal developments in recent years have reduced the potential for this.

21. A trust can be defined generally as a legal relationship that is set up – either *inter vivos* or on death – by a person (the *settlor*) when the assets have been placed under the control of another person (the *trustee*) for the benefit of one or more persons (the *beneficiary*) or for a specified purpose. There are several characteristics of a trust that set it apart from other legal relationships:

- The trustee becomes the legal owner of the trust property.
- The assets held in trust are separate and do not constitute part of the trustee's own estate.
- The trustee has the authority and the obligation to manage, employ or dispose of the assets held in trust in accordance with the terms of the trust and any special duties imposed by law.[10]
- The beneficiary has equitable property rights with regard to the trust property (depending on the jurisdiction and the nature of the trust[11]).

22. Sometimes a trust may involve a fourth person (the *trust protector*), who is appointed by the settlor to ensure that the trustee manages or disposes of the assets held in trust according to the settlor's intentions.

23. In theory then, there are three elements which must be present in order to have a valid trust. (1) It must be possible to identify clearly the subject (the assets or property) of the trust. (2) It must be clearly stated by the settlor that his or her intention is to place these assets or property in trust and not simply to give them as a gift. A *trust deed* is usually prepared for this purpose. (3) It must be possible to identify who the intended beneficiaries are. The beneficiaries will usually be indicated in the trust deed; however, in certain instances they may only be indicated as a general category and not by name. There is often then a *letter of wishes* prepared by the settlor setting out his wishes as to who is to benefit from the trust and under what conditions.

24. Trusts are, however, sometimes used as an element in schemes to facilitate or hide illicit activity, including money laundering. Given the private nature of trusts, in some jurisdictions they may be formed with the intention of taking advantage of strict privacy or secrecy rules in order to conceal the identity of the true owner or beneficiary of the trust property. They are also sometimes

---

9 See the *FATF Review to Identify Non-Cooperative Countries or Territories: Increasing the Worldwide Effectiveness of Anti-Money Laundering Measures*, 22 June 2000, for further discussion of this initiative.

10 See also the *Convention on the Law Applicable to Trusts and on Their Recognition*, The Hague, 1 July 1985 ("The Hague Convention on Trusts of 1985").

11 In some jurisdictions, the beneficiary of a trust does not have specific concomitant property rights over the trust property but may take legal action against the trustee to force the execution of the trust as intended by the settlor. In this respect, the beneficiary is acting to enforce an irreducible core of obligations owed by the trustee to the beneficiary and enforceable by him which is fundamental to the concept of a trust.

used to hide assets from legitimate creditors, protect property from seizure under judicial action, or to mask the various links in the money flows associated with money laundering or tax evasion schemes.

c. Implications for money laundering

25. There appears to be limited potential for trusts to be used at the initial or placement stage of the money laundering process. Indeed, criminally derived funds would normally already have to have been inserted into the financial system before such assets could be placed into a trust. At the layering and integration stages of money laundering, however, there is greater potential for the misuse of trusts. Once the illegal proceeds have already entered the banking system, trusts can be exploited to further confuse the links between these proceeds and the illicit activity that generated them. This process may be even more effective if it is carried out in a number of countries and through legal professionals who are then able to claim some sort of professional secrecy.

26. It should be pointed out that a trust is not the same as a company or other form of corporate entity. When a company is established, it has its own "legal personality" that is separate and distinct from the natural persons that serve as directors or shareholders. Property held by a company is owned by the company as a legal person and not individually by the company directors or shareholders. Property held in trust, on the other hand, is legally owned by the trustee and no longer by the settlor nor by the beneficiary. Therefore, when dealing with certain trusts, the work of an investigator may be further complicated by the fact that the trustee may be a legal person (a trust company for example), and the beneficiary or beneficiaries may also be trusts (or corporate entities). Establishing whether there are real persons behind the legal arrangement and that the trust is a sham is a difficult if not impossible task.

27. Furthermore, trusts differ from corporate entities in that they generally have no registration requirement or central registry, and there is usually no authority responsible for oversight of such legal arrangements. Some jurisdictions now have introduced legislation for the regulation and supervision of trust companies, trustees, company incorporators, company administrators, and company directors very much along the lines of the regulation and supervision of banks. In some jurisdictions, there is also a legal requirement under all crimes money laundering legislation to file suspicious transaction reports, and information on the identities of the settlor or the beneficiaries of a trust is obtainable. In some jurisdictions that recognise trusts there is, however, no requirement to disclose the identities of the settlor or the beneficiaries of a trust even when the trust might be associated with some sort of suspicious financial activity.

28. The payments to the beneficiaries of a trust could be used in the money laundering process, as such payments do not have to be justified as a payment for a transfer of assets or service rendered. Some trusts are created, however, with what appears to be the intention of preserving the anonymity of the settlor or beneficiaries. In the so-called "black hole" or "blind trust", which is possible to establish in some jurisdictions, neither the real purpose of the trust nor its beneficiaries can be identified from the trust deed itself. The real beneficiaries might be referred to in a letter of wishes from the settlor; however, the existence of such a document may not be voluntarily acknowledged by the trustee.

29. In recent years, changes to the trust laws in many jurisdictions have helped to increase their attractiveness for concealing the identity of the persons involved in such legal arrangements and thus facilitating the work of money launderers and the perpetrators of other criminal activity. The trusts established using these new laws often bear little or no resemblance to the trusts formed in traditional common law contexts. Some jurisdictions now offer what are termed "asset protection trusts" that may permit the settlor to keep control over the trust assets by being named as the beneficiary of such an arrangement. Other jurisdictions have permitted trusts to be formed with what are known as "flee clauses". These provisions in the trust document provide for the automatic transfer of the trust to another jurisdiction if the trust becomes the subject of any sort of enquiry.

Example 4: A trust is used for laundering the proceed of alcohol smuggling

Some years ago a national of Country A was convicted of smuggling a huge quantity of alcohol. Just a small part of the proceeds were confiscated. The police found documents showing that his companies in Country A had mortgage loans from a company owned by a trust from a small island jurisdiction (Country B). After the conviction, the FIU in Country A learned that it was the convicted person and later his common law wife who were the beneficial owners of the company. With assistance from the office of the public prosecutor in Country B, the FIU got information which showed that the company received money from a bank account in a third country (Country C). It was suspected that the proceeds from the smuggling had been transported as cash to the Country C bank, then to the trust in Country B and finally back to Country A as "mortgage loans". It was clear that neither the companies nor the convicted person or his common law wife had paid any instalments.

Example 5: The difficulties for investigations involving trusts

In a recent case, an significant sum of money was to be invested by a trust into a company with financial difficulties in Country D. The trust was identified by its name and represented by a natural person, a member of a law office, acting as the trustee with all of the powers associated with this function. Up to this point, this proposed dealing did not appear to be suspicious in the eyes of the bank responsible for managing the transaction. However, the FIU in Country D was aware of this suspicious nature because then an offshore company appeared in the financing process. The company was controlled by persons known to be involved in suspect activity and for whom it was impossible from the start to determine if they also were behind the trust. The absence of any registration of the trust and of any information on its settlor or beneficiaries, other than those stated by the trustee, made the investigation considerably more complicated.

d. Possible counter-measures

30. This year's typologies exercise was the first to focus on trusts as another legal mechanism that could be misused for money laundering purposes. In many ways, this use is similar to and associated with the role of corporate entities and company formation agents discussed in earlier typologies studies.[12] Consequently, the actions proposed by the experts this year for dealing with trusts should also be viewed in the larger context of confronting the misuse of all legal mechanisms for money laundering purposes, increasing transparency with regard to such formations, more closely ensuring the integrity of the professionals involved in the creation of these mechanisms, and working toward some universal standards that could preclude the establishment of systems in certain jurisdictions that facilitate and protect such misuse. Some of the specific possible actions that could be taken to help money laundering investigations involving trusts include:

- Establish regulation and licensing of professionals involved in trust formation. Creating such a system would necessarily mean requiring these professionals to apply the same anti-money laundering preventive measures as those employed by financial institutions (i.e., customer identification, record keeping, reporting of suspicious transactions) and would need to rely on appropriate inspection procedures to ensure compliance with such rules.

- Regulate the form of trusts. Establishing norms in this area could mean imposing a standardised documentation requirement for trusts that could vary according to the types of trusts and might also include abolishing or banning certain types of particularly abusive forms of trust (i.e., the "blind" or "black hole" trusts, etc.) or certain harmful aspects such as "flee clauses" or the possibility for a settlor to retain control of assets (i.e., the asset protection trust).

- Impose a registration requirement for trusts. Setting up a trust registration requirement would guarantee a degree of transparency regarding these legal arrangements; however, it might also encounter a great deal of resistance from certain jurisdictions for both practical and ethical reasons. A few jurisdictions already require the registration of trusts with a central trust registry

[12] See the FATF-X (1998-1999) and FATF-XI (1999-2000) typologies reports for further discussion of these two issues.

office, primarily for fiscal reasons. Most jurisdictions in which trusts exist do not have registration of these legal arrangements, however. A compromise solution might be to require recording of trusts in registries to which only financial institutions and government investigative and regulatory authorities might have access. Another possibility would be to require registration only for trusts having certain characteristics (involving assets above a certain value or where the trust is established for specific commercial purposes, for example).

(iii) Lawyers / Notaries, Accountants and Other Professionals

a. General

31. Lawyers, notaries, accountants and other professionals offering financial advice have become the common elements to complex money laundering schemes. This trend is mentioned by almost all FATF members. Previous typologies exercises have cited their often key role in helping to set up such schemes, particularly in the framework of company formation agents as discussed during last year's exercise. It was felt worthwhile, therefore, to give some specific attention to the professions involved given the complexity and some of the sensitivities of dealing with their role in money laundering.

b. Nature of involvement of these professions: the "Gatekeepers"

32. The continuing effort by governments to combat money laundering has made the work of the money launderer more difficult. In part as a means of circumventing money laundering counter-measures, launderers have had to develop more complex schemes. This increase in complexity, the FATF experts have observed, means that those individuals desiring to launder criminal proceeds – unless they already have specialised professional expertise themselves – must turn to the expertise of legal professionals, accountants, financial consultants, and other professionals to aid them in the movement of such proceeds. If one looks at the types of assistance that these professionals may provide, it is apparent that some of these functions are the gateway through which the launderer must pass to achieve his goals. Thus the legal and accounting professionals serve as a sort of "gatekeeper" since they have the ability to furnish access (knowingly or unwittingly) to the various functions that might help the criminal with funds to move or conceal.

Professional Services Provided by . . .

Lawyers	Accountants
Legal advice	Financial advice
Advocacy	Audit practice
Wills / probate	Tax advice and tax structuring
Property transactions	Bookkeeping
Investment services	Company formation
Trust	Company administration
Company formation	Trust
Company administration	Property transactions
Introduction to banks	Introduction to banks

33. Not all of these functions have the same utility to a potential laundering operation. The functions that are the most useful to the potential launderer include:

- Creation of corporate vehicles or other complex legal arrangements (trusts, for example). Such constructions may serve to confuse the links between the proceeds of a crime and the perpetrator.
- Buying or selling of property. Property transfers serve as either the cover for transfers of illegal funds (layering stage) or else they represent the final investment of these proceeds after their having passed through the laundering process (integration stage).
- Performing financial transactions. Sometimes these professionals may carry out various financial operations on behalf of the client (for example, cash deposits or withdrawals on accounts, retail foreign exchange operations, issuing and cashing cheques, purchase and sale of stock, sending and receiving international funds transfers, etc.).
- Financial and tax advice. Criminals with a large amount of money to invest may pose as individuals hoping to minimise their tax liabilities or desiring to place assets out of reach in order to avoid future liabilities.
- Gaining introductions to financial institutions.

34. In some of these functions, the potential launderer is obviously not only relying on the expertise of these professionals but is also using them and their professional status to minimise suspicion surrounding their criminal activities. A solicitor representing a client in a financial transaction or providing an introduction to a financial institution lends a certain amount of credibility in the eyes of the transactor because of the ethical standards presumed to be associated with the work of such professions.

c. Potential remedies

35. Several countries within the FATF have already decided to include certain non-financial professionals under the requirements imposed by their anti-money laundering laws and regulations. In particular with such professions, these countries emphasise customer and beneficial owner identification, record keeping and suspicious transaction reporting. The range of professions covered varies. Some have been able to include all professions at risk of becoming money laundering facilitators (solicitors, notaries, accountants, real estate agents, financial or tax consultants, etc.); while others have only extended the requirements to certain professions.

36. There remain a number of obstacles to bringing the various "gatekeepers" under anti-money laundering obligations, in particular the legal professions. Often these professions are not the principals involved in a money laundering operation and are therefore unaware of how their advice or legal mechanisms are ultimately used. Even if this is sometimes correctly or incorrectly perceived as wilful blindness on the part of the professional, there is the additional factor that many legal professionals see compliance with anti-money laundering requirements as conflicting with the privilege of confidentiality in lawyer / client communication. Indeed, in some jurisdictions, there are legal prohibitions on divulging such information, and the prohibition extends to all communication regardless of whether in relates to the advocacy function or not. Moves to include the legal professions under anti-money laundering requirements necessarily confront significant resistance from these professions and privacy advocates in such jurisdictions.

37. It is worth mentioning that within the European Union (EU), acceptance of the need to include "gatekeepers" under anti-money laundering obligations appears to have gained ground with the proposed revisions to the EU anti-money laundering directive[13]. A modification to the directive will require a broad range of professions (including "notaries and other independent legal professionals", as well as accountants and auditors) to abide by anti-money laundering rules when they assist in the planning or performance or act on behalf of their clients in the conduct of certain

[13] Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering.

financial or commercial activities.[14] This solution, if endorsed by the European Parliament, will then have to be transposed into the domestic laws of the 15 members of the European Union. Its focus on the functions performed, as clearly distinct from the advocacy role of legal professions, is an approach that might be feasible elsewhere.

Example 7: Lawyer assists in setting up a complex laundering scheme

This case involved 19 individuals in the medical service industry, one being both a lawyer and an accountant. This dossier submitted for prosecution contained 123 violations involving conspiracy, false claims, wire fraud and money laundering. The false claims involved fictitious patient claims and claims for services which were not provided.

The two primary subjects employed the lawyer's services to set up four interrelated shell corporations as the controlling entities. In addition, eight nominee corporations were created to generate fictitious health care service records reflecting in-home therapy and nursing care. Health care providers including therapists, registered nurses and physicians operated the nominee corporations. To keep the health care billing, tax return filings and bank account records synchronised, the two main subjects relied on the lawyer / accountant defendant.

In excess of USD 4 million was laundered through bank accounts in cities of the north and south-east of the country and through suspected offshore accounts. Numerous accounts were created at four or five separate banks for purposes of amassing and moving these funds. Cashier's cheques often were purchased and even negotiated through the lawyer/accountant's trust account for concealment of property acquisition. This defendant was sentenced to two years in exchange for his co-operation.

Both primary defendants were ordered to forfeit real and personal property, including the USD 4 million and purchased property. They received five- and two-year prison sentences respectively. Two additional related case defendants (one being an elected official), laundered an additional USD 2 million and were charged with 33 violations of the law in a separate case. They were ordered to forfeit USD 95,000 in currency. The former elected official received a five-year prison sentence.

Example 8: Failure to disclose suspicious activity by legal professional

A firm of lawyers was asked by a client to assist in the arrangement of a substantial loan to a third party. The solicitor tasked with assisting the client was instructed to request some form of guarantee from the third party. The third party initially sent an insurance bond, which turned out on inspection to be worthless. The lawyer requested another guarantee and received share certificates in an foreign company; however, these proved to have been stolen. The lawyer made a third request and received some prime bank guarantees with a value far in excess of the initial loan. The lawyer was then asked by the first client to assist in the sale of the prime bank guarantees by certifying as to their authenticity, which he proceeded to do using letterhead stationery from the law firm. Despite the suspicious circumstances, the lawyer made no disclosure to law enforcement and, at the time of writing, left his firm potentially exposed due to his willingness to "certify" documents often known to be used in international frauds.

[14] Draft text as currently being considered (text as of 29 November 2000):

Member States shall ensure that the obligations laid down in this Directive are imposed on the following institutions :

…

5. notaries and other independent legal professionals, when they participate, whether :

(a) by assisting in the planning or execution of transactions for their client concerning the

(i) buying and selling of real property or business entities;

(ii) managing of client money, securities or other assets;

(iii) opening or management of bank, savings or securities accounts;

(iv) organisation of contributions necessary for the creation, operation or management of companies;

(v) creation, operation or management of trusts, companies or similar structures;

(b) or by acting on behalf of and for their client in any financial or real estate transaction

…

Example 9: Financial consultant sets up laundering operation through shell companies

A financial consultant based in a European financial centre (Country A) provided expertise in setting up "shell" companies in an neighbouring country to act as "missing traders" (businesses that exist only on paper and do not account for any excise or taxes) to disguise the origins of profits from smuggled goods sold on the black market of Country B. Bank drafts were paid from accounts of shell companies in Country B to bank accounts at the financial centre held in the name of further Country B businesses. The funds were finally moved to the Middle East and used in commodity transactions for final legitimisation prior to return to the Country B. Involvement and advice of financial professionals throughout was vital to the laundering operation.

Example 10: Failure to disclose suspicious activity by financial professional

In a recent major loan sharking investigation in an Asian country, an accountant responsible for auditing the accounts of a company, which had received crime proceeds laundered through a neighbouring State, failed to report any suspicious transactions. Investigators found obvious discrepancies in the company's account records which should have alerted the accountant, such as unexplained large-summed payments from and to the Director (who was the mastermind of the loan sharking syndicate), the fact that no delivery or warehousing expenses were ever booked for the trades purportedly conducted, and that in one instance the date of delivery of the "goods" to the buyer actually predated the date of acquisition by the seller. The accountant, when questioned, stated that he failed to note any suspicion because he only looked at the year-end figures for the purposes of certification of the accounts.

Example 11: Laundering operation is set up by accounting firm

In March 2000, the Director of an insurance company from a country in Asia (Country C) defrauded the company of USD 90 million by purporting to have purchased bonds of the same amount. The proceeds were paid through two companies registered in a Caribbean island country (Country D) and holding bank accounts in another Asian country (Country E). The Country D companies and the bank accounts had been set up and run by an Asian accounting firm for the offending Director. The USD 90 million was firstly paid to one of the Country D companies, then transferred to the other, and then back to Country C to a third company also owned by the Director, all in the same day. The Director has since been arrested by the Country C Police and is in custody pending trial.

The accounting firm failed to note the U-turn movement of the funds as suspicious and thus did not make any disclosure. Moreover, in September 2000, staff of the accounting firm became aware of the Director's fraud and that he had used the Country D companies and accounts set up by their firm to launder the funds. Still the management committee of the accounting firm did not make any disclosure to the authorities. They limited their action to ascertaining if they could be liable in any way for negligence. The four-member management committee of the accounting firm (all senior accounting firm partners) and the partner who handled the account have all been arrested for an offence of failing to make a disclosure.

(iv) The Role of Cash vs. Other Payment Methods in Money Laundering Schemes

a. General

38. When the FATF Forty Recommendations were first issued in 1990, the focus of many of its preventative measures was on detecting money laundering at the cash proceeds stage. Many anti-money laundering systems put into place since that time have had that same emphasis on recording or reporting large cash transactions. Given the evolution of money laundering methods and the financial sector during the past ten years, examining the current and future importance of cash (vis-à-vis other payment methods) in money laundering appeared to be appropriate at this time.

Example 12: Currency conversion conceals laundering operation

Using various identities, the resident of a neighbouring country, went on several occasions to several tellers of a branch of a bank in order to exchange the equivalent of approximately USD 11,000 into a third country currency.. The banknotes presented were strangely coloured and had a bad odour as if they had been hidden and stored without protection from environment over a long period. The Prosecutor's Office managed to block a part of the funds involved. The investigation

revealed that the individual was known for, among other things, bank hold ups and armed robbery as a member of a criminal organisation, with the proceeds of these crimes being the same currency as the banknotes presented to the bank tellers.

b. Cash proceeds

39. According to the experts in this year's typologies exercise, cash remains the major if not primary form in which illegal funds are generated today. One FATF jurisdiction noted that in that jurisdiction there is currently an increased demand for banknotes which seems incongruous with the general shift of the public to non-cash means of payment. One explanation could be the continuing growth of the underground economy in other countries where banknotes are circulating.. Using the measure of suspicious transaction reports (STRs), two FATF members have found that the number of such reports dealing with cash makes up between two thirds and three quarters of all reports filed. Another FATF jurisdiction also has noted a rise in cash related STRs despite ever decreasing reliance on cash by the general public. It observes, however, that this change could be attributed to the fact that as cash transactions become less common for ordinary transactions, those cash transactions that do take place are more likely to draw attention from financial institutions.

40. Cash proceeds are usually found at the beginning of the laundering process, that is, at the placement stage, although some of the experts have observed laundering schemes in which proceeds are converted back to cash at some later point in the process in order to break the paper trail. To place the proceeds into the financial system, launderers use many of the tried and true methods, including deposits directly into bank accounts (usually through structured transactions and ATMs); the purchase of certain types of assets: real property, vehicles, jewellery, furniture, appliances, and collectibles (antiques, coins, stamps, etc.); and the commingling of legal and illegal cash proceeds (which are then deposited into bank accounts as ostensibly legitimate cash proceeds).

Example 13: Cash laundered through purchases at auctions

A sophisticated criminal group importing cannabis resin into the country was arrested and approximately USD 2.5 million in assets were restrained. One method they used to launder their money was through cash purchases of large items at a public auction. The subjects purchased a house and boats, and the extent of the inquiry by the public auction regarding the source of the funds was satisfied by the suspect providing proof of a place of work.

41. Despite the anonymity that proceeds in cash form may provide to the launderer, it is still not the preferred form for launderers and criminals. In order to circumvent anti-money laundering measures in place in FATF countries (and increasingly in other countries as well), launderers must move cash proceeds to locations where they may somehow be inserted into the financial system. In this respect, cash movement – especially across national borders – seems to be becoming a more widespread and necessary element for large scale laundering schemes. The use of large denomination banknotes is important in reducing the bulkiness of these physical cash movements. Canada is one country that has recently decided to cease the issue of the $1000 (approximately USD 650) bank note and to withdraw existing notes from circulation as part of its response to money laundering and organised crime.

42. The utility of cross-border reporting requirements was mentioned by the FATF experts and delegations as a means of detecting some movements of criminal proceeds. Several FATF member jurisdictions already have such systems in place, and a number of others either are considering or already plan to implement such systems. Recent studies conducted in Europe – Project Goldfinger in the Baltic Region and Project Moneypenny in several European Union airports – appear to reinforce the need for tracking cash movements across borders. In the three-month period of the Goldfinger operation, the various customs and other enforcement authorities detected USD 78.2 million in approximately 2,500 movements of cash among the ten participating jurisdictions. Although there

were indicators of criminal activity in only a small number of the shipments[15], the operation showed the significance of such flows of funds that might otherwise have gone undetected.

43. Experts from non-FATF countries who participated in this year's exercise pointed out that cash transactions remain the primary form of financial transaction in many regions of the world outside the FATF membership. As in some FATF countries, non-traditional financial institutions (such as bureaux de change and money remittance services) often play a significant role in financial systems of certain countries, and these businesses are generally highly cash-oriented. Cash movements within countries or across borders in some regions do not attract attention, and some jurisdictions would have a great deal of difficulty in imposing any sort of controls of such movements. Nevertheless, it is important from the perspective of these countries to continue focusing on criminal proceeds in the form of cash.

Example 14: Non-resident bank accounts move money offshore

In one European country (Country A), transactions involving non-residential accounts of the companies from off–shore areas can be divided in two groups according to the form of the account and the technique used: (1) cash operations in connection with non-residential accounts and (2) cashless operations on non-residential accounts.

In connection with cash operations through non-residential accounts, the FIU in Country A had a recent case which dealt with two companies registered in two other European countries. Foreign citizens, who were authorised for representation of companies, opened non-residential accounts at two Country A banks. In the period of 20 months, cash was deposited on mentioned accounts in total amount of over USD 8,000,000. Later they brought cash from abroad and avoided reporting by the customs authorities of Country A. Generally, the cash was in small denomination bank notes. As soon as the cash deposit was executed, they gave a money order to the bank for a cashless allocation of money to the credit of numerous foreign companies registered in five other countries. The legal basis for these transactions consisted of invoices from companies engaged in the selling of tobacco products and alcohol that were issued for the payment of large quantities of cigarettes. In connection with these transactions, the Country A FIU found that the money originated from tax fraud against European Union interests and from the smuggling of cigarettes. With the help of forged documentation, the perpetrators misrepresented to the Country A customs authorities that the cigarettes were exported from European Union countries to the East. In fact, the cigarettes were sold on the black market in several European countries. Non-residential accounts were opened in Country A with the single purpose of laundering the illegal funds derived from the sale of smuggled cigarettes. Deposits into the accounts of off-shore companies were made with the attempt to cover real origin of money, to remove links from the perpetrators of predicate offences and also for payment of new quantities of cigarettes.

Example 15: Cash narcotics proceeds smuggled to a free trade zone

In one narcotics consuming country (Country B), bags of money which were the product of illegal drug sales, in amounts of approximately USD 700,000 weekly, were handed over to two individuals. The total amount involved is estimated to have been USD 13 million. The money was given by the individuals to jewellery stores in the city where the illegal proceeds had been generated. The stores in turn deposited the funds into various banks in amounts just under the STR reporting threshold. With the funds from the deposits, the jewellery stores bought cheques whose beneficiary was a firm that belonged to one of the individuals in the free trade zone (FTZ) of a nearby country (Country C).

In the FTZ, the cheques were used by the firm to pay for imports from an important narcotics producing country (Country D), and a commission was obtained for this service. Also, importers from Country D settled their export transactions by making payments to the enterprises indicated by the second individual. The cheques were deposited by various companies located of the FTZ into banks located within the zone, as payment for real and legitimate purchases from importers from Country B.

One of the individuals was prosecuted and convicted in Country B for money laundering, with a reduced sentence for having co-operated with the authorities. The second individual was convicted for money laundering in Country C. The FTZ business that had been used in the operation was closed by the authorities and the physical goods that it contained were confiscated by the Government. There was no charge made against banks.

[15] Five criminal investigations were developed from the reports, including one conviction for money laundering.

c. Wire transfers and other cashless forms of payment

44. It was agreed by the experts that, despite the continuing need to focus on the cash proceeds in money laundering operations, there was still some need to look at these other forms of payment that often play the most important role at later stages of the process. Some countries appear to have had some success at deterring the placement of cash proceeds directly into their financial systems, or, because of the size, the development, or the sophistication of their financial system, they have become more important simply as a transit point for laundered funds. Additionally, some types of criminal activity may actually be generating proceeds in a non-cash form from the beginning (for example, investment fraud). Both transit movements and proceeds generated in electronic form are difficult to detect given what some experts perceive as an overemphasis on cash operations.

45. In some laundering operations, wire transfers are made in close connection to cash deposits. However, since wire transfers frequently take place at the layering stage, there is often little to distinguish a suspicious transaction from others. Investigators must rely on ties to other factors, such as STRs, cross-border reporting or information contained in SWIFT[16] messages used in interbank transfers. The experts were therefore also concerned about the continued lack of uniformity in identifying the originator of wire transfers (through the SWIFT messaging system). Although for a number of years these messages have provided a field for indicating the originator of funds, the field is not mandatory.

Example 16: Structured international funds transfers

This operation was initiated after the automated monitoring system of the FIU in a country of the Asia / Pacific region (Country E) identified structured international funds transfer instructions to the value of USD 593,430 to another Asia / Pacific country (Country F) over a three-month period. Other information confirmed that persons remitting money overseas were structuring transactions to avoid reporting of significant cash transaction reports.

Investigators discovered that false names had been used when making the international funds transfer instructions, except in one instance. A search of relevant records identified this person and surveillance was initiated upon the suspect. This surveillance revealed a number of people, all from one address, making numerous structured cash transactions at various banks. These people were also observed going to several businesses owned by the same corporation. It was revealed that this corporation was owned by a relative of the principal target who was suspected of being associated with an earlier importation of heroin into Country E.

Investigators also identified another person who had recently arrived in Country E from yet another country of the region (Country F). It was suspected that one residence identified by investigators was used as a 'safe house' for the purpose of heroin distribution. In December of that year a package containing a quantity of heroin was delivered to the address, resulting in one arrest and the seizure of 4.1 kilograms of high purity heroin.

The operation concluded with three arrests that were all successfully prosecuted. The co-ordinator of the foreign nationals making the international funds transfers was also arrested and charged with being knowingly concerned with the importation of heroin. She was found guilty and sentenced to 10 years imprisonment.

d. Electronic purses, Smartcards, and WAP technology

46. New payment technologies such as the electronic purse and Smartcards have been considered in previous FATF typologies work as these systems were first being developed and tested.[17] A few of the FATF delegations mentioned these technologies as still being of concern for the future. However, the implementation of such systems has remained relatively limited up to now, and no new vulnerabilities have therefore been identified in this regard.

[16] *Society for Worldwide Interbank Financial Telecommunications*, the leading international payment and messaging network.

[17] See *FATF-VIII Report on Money Laundering Typologies, 1996-1997*.

47. A few FATF members mentioned the introduction of WAP technology as a potential means of facilitating money laundering operations and something worthy of future examination by the FATF. WAP technology permits direct access to Internet through mobile phones. The implications for money laundering will likely be similar to those already cited for on-line banking and other Internet related activities. This technology has not yet been broadly introduced due to the lack of available bandwidth for digital telephone networks and the small size of the screens on current portable phones. It appears, therefore, that a closer examination of money laundering risks specific to this new technology will have to wait until it has been put into widespread use.

(v) Terrorist Related Money Laundering

48. This year the FATF experts on typologies undertook to examine the means by which terrorists conceal or move funds in support of their operations and how these methods might be different from those used by other criminal groups. One objective of this discussion was to determine whether the distinction between legal and illegal sources of funding has an effect on the ability of countries to use anti-money laundering measures to detect, investigate and prosecute potential terrorist related money laundering.

49. As part of examining this subject, it is important to understand the sources of funding used by terrorist groups to finance their operations. Among some of the major sources are:

- Drug trafficking
- Extortion and kidnapping
- Robbery
- Fraud
- Gambling
- Smuggling and trafficking in counterfeit goods
- Direct sponsorship by certain states
- Contributions and donations
- Sale of publications (legal and illegal)
- Funds derived from legitimate business activities

With the decline in direct state sponsorship of terrorism, terrorist groups have increasingly resorted to criminal activity to raise the funds needed to support their activities. Even with a cursory look at the list of these activities, it is evident that – except for the last four – there is little difference in the sources currently used for both terrorist and organised crime groups.

Example 17: Terrorist group uses same laundering methods as organised crime

The money laundering method of the regional liberation movement is identical to that of traditional criminal groups; first, the money is deposited into various banks of the region, where the issue of certificates of deposit takes place. Then, these certificates are deposited through intermediary companies in numbered accounts in banks at offshore tax havens, which may only be accessed by code. In the third phase, some of this money is transferred to several European banks from which cheques or payment orders are issued from differing current accounts. Finally, the money is transferred to accounts without arousing suspicion in the territory where the liberation movement is active.

50. As for the methods used by terrorist groups to launder funds derived from these criminal sources, the experts provided examples which appear to indicate that the same laundering methods are used by both terrorism and organised crime. Although terrorism and organised crime might use the same laundering methods, the two forms of criminal activity differ in their ultimate motives. Unlike drug traffickers and other organised crime groups that primarily seek monetary gain, terrorist groups usually act to further non-financial goals. Certain experts brought up the point that, despite the similar laundering methods and differences in motivation, this activity might not constitute money

laundering per se if the source of the funding is not from criminal activity (for example, if the funds were derived from contributions or donations). If no connection could be shown between the funds and a criminal act that generated them, then these jurisdictions might not be able to assist the investigation or target the funds using anti-money laundering laws.

51. All experts agreed that terrorism is a serious crime which should be targeted along with the other serious crimes that serve as the underlying offences for money laundering. There was not agreement, however, on whether anti-money laundering laws could (or should) play a direct role in the fight against terrorism. Some of the experts were of the opinion that terrorist related money laundering indeed constitutes a distinct subtype of money laundering and should therefore become a specific focus of anti-money laundering measures. Other experts remained unconvinced believing that the focus of money laundering counter-measures on serious crime (including terrorism) is sufficient and that further refinement of specific anti-terrorism measures should take place elsewhere.

Example 18: Unexplained funds turn out to be terrorist related

A current case in a European country (Country A) provides an interesting example of the financing of terrorists acts. In August 1982, a female individual opened an account at a bank in Country A. In September 1984, a male individual was given authority to sign for this account. Recently, the deposit in the account amounted to approximately USD 7 million.

The male is a known high-ranking member of an international terrorist organisation and was probably responsible for the financial transactions of the organisation. He is believed to the husband of the female individual mentioned above, although she denies it.

Between 1991 and 1995 both individuals attempted several times to gain access to this account from abroad. In October and November 1999, the alleged account owner instructed the bank to transfer USD 2 million to another bank account. The fact that the signature of the female appeared not to be identical with the signature when the account was opened gave rise to suspicion of fraud, and a complaint was filed.

In January 2000, a court issued an arrest warrant for the female suspect, which was executed the very same day. During her questioning, she was unable to provide a plausible explanation for the legal origin of the funds. The investigations of the FIU in this respect could not completely clarify this either, but there is reason to suspect that the monies are from the terrorist organisation with which the male suspect is associated.

In April 2000, the first hearing in the case against the female suspect took place before a regional court for suspicion of membership in a criminal organisation. The court ordered to set her free for a bail of USD 40,000. The proceedings have meanwhile been adjourned several times, and the account has been temporarily frozen.

Example 19: Terrorists launder smuggling proceeds

A wide ranging, joint criminal and financial police investigation in Country B into national level cigarette smuggling, involving a suspected terrorist cell, led to the arrest by authorities of 18 individuals, and the search of 18 residences and businesses. These individuals, including seven suspected supporters of the same terrorist cell, were subsequently charged with: marriage, visa and other types of immigration fraud and related bribery and conspiracies; conspiring to smuggle contraband cigarettes; and conspiring to launder money. Many of the defendants continue to be detained prior to trial, while the investigation continues.

As noted, at least seven of the defendants are suspected members of, or sympathetic to group mentioned above, a foreign terrorist organisation designated as such pursuant to Country B's anti-terrorism law. These seven defendants appear to be providing material support or resources to the terrorist group in violation of Country B laws. The defendants' material support activities continues to be investigated and, if appropriate, Country B will bring additional charges alleging that the defendants knowingly provided material support.

More specifically, the current charging document alleges that seven of the defendants entered into fraudulent marriages with Country B citizens in order to obtain permanent resident status which would permit them to remain indefinitely in Country B. Having arranged for their continuing presence in the country, for a four-year period, several of the defendants smuggled large quantities of contraband cigarettes by taking advantage of differing tax rates among various jurisdictions. During the

same period, these defendants laundered the funds involved in and derived from the conspiracy through various bank and credit card accounts.

According to the formal charges, many of the individuals involved and their associates gathered each week in one Country B city for prayer meetings. The business of the terrorist group was also discussed at these meetings and fiscal contributions to the organisation were solicited from the group. Those who participated in the cigarette smuggling scheme would commingle a portion of the funds that were the proceeds of that activity with the funds collected as contributions. Some of the individuals involved would then arrange for the combined criminal proceeds and the collected funds to be sent, usually by courier, to other cells of the group located abroad.

The defendants are each facing substantial periods of incarceration, criminal fines and asset forfeiture. Among the assets that may be subject to forfeiture are: two residences, a petrol station; an undetermined amount of currency; five automobiles; and 30 bank accounts. Four of the defendants who participated in fraudulent marriages have pled guilty. At the request of the defence, the trial of the remaining defendants will likely be delayed until April 2001.

III. MONEY LAUNDERING TRENDS

(i) Sources of illegal funds

52. The most important source of criminal proceeds laundered is still represented by those proceeds derived from narcotics trafficking, according to the FATF experts. Various fraud schemes continue to be the next most common criminal activities generating funds for laundering, and this trend appears to be increasing both in the number of cases and the amount of money involved. One country estimates that funds involved in investment fraud within its jurisdiction total some USD 22.5 million annually. Smuggling, embezzlement and other types of theft, corruption, and tax evasion remain important sources for laundered funds. Trafficking in human beings was noted as a growing source of illegal funds in last year's exercise; this year, the trend appears to have spread to other FATF jurisdictions.

53. Mention should be made of the increased effort on the part of anti-money laundering authorities – especially national financial intelligence units – to capture and analyse data on the nature and extent of money laundering within their jurisdictions. Much of the analysis for this year's typologies exercise is based on the assessments of the individual FIUs, which in many cases provided extremely detailed analysis of STRs and other related data. Although this material provides only part of the picture of the money laundering situation in any one country, it is quite a significant part. These detailed national analyses, as they become more common, will likely help to expand trend analysis in the framework of the FATF typologies exercises.

(ii) New methods or techniques and significant changes in trends

54. In general, FATF countries see the same money laundering methods and techniques that have been observed and described in previous FATF typologies exercises. If there are changes in these trends, they are primarily the observation of a new method or technique that had not yet been found in a particular jurisdiction or the relative increase in reporting of certain types of suspicious activities. Much of the information and examples provided by the experts for this year's typologies work focused on the five specialised topics. This material has already been incorporated into the discussion of those topics earlier in this report. The observations presented here will therefore be limited to other areas not already highlighted in this earlier treatment.

55. Alternative remittance systems and trade related activities[18] continue to serve as both vectors and a cover for certain money laundering schemes. Australia mentioned that it finds itself

[18] See *FATF-XI Report on Money Laundering Typologies, 1999-2000,* for more discussion of these money laundering methods.

increasingly used as the "host" for such activities, and other countries – the United States and France in particular -- provided case examples having direct or indirect indicators of such activity.

Example 20: Underground bank launders South Asian funds

An FIU was alerted to atypical financial movements that affected bank accounts of an individual of Asian origin, into whose bank account cash was regularly deposited. The deposits, carried out by a close friend exceeded USD 2.6 million in one year. These sums were then transferred to a second account opened by the suspect in his country of origin.

Analysis of the case showed that the person in question was acting as a "banker" for the Asian community situated in several European Union countries to which he provided cheques for cash in the currency of countries of destination for the funds. The main actor in this case is suspected to be masterminding a laundering scheme for proceeds of heroin trafficking controlled from abroad.

56. Several countries reported similar schemes involving cash deposits – often structured to avoid triggering reporting requirements – which are closely associated with wire transfers. These transactions take place either through ordinary financial institutions or money remittance services. In Australia, the schemes often make use of non-nationals, and funds are generally sent to the Southeast Asia region. Belgium has observed series of money laundering operations which are believed to be primarily linked to funds derived from prostitution and human being trafficking. France mentioned similar type schemes involving narcotics proceeds and connections to Eastern Europe.

Example 21: Foreign nationals used in laundering operation

An investigation undertaken by a law enforcement agency revealed a suspected money launderer for a narcotics syndicate, utilising foreign nationals. The foreign nationals had legally gained entry to the country under a particular category of visa. The suspected money launderer, a foreign national herself, utilised fellow countrymen to remit funds overseas via telegraphic transfers, in amounts under USD 5,400.

Example 22: Tourists launder stolen and altered cheques

An investigation undertaken by a law enforcement agency highlighted the existence of a highly organised Southeast Asian syndicate utilising tourists to launder stolen and altered cheques. The tourists would be brought to the country and advised how to open bank accounts in their real names. Once the accounts were opened, the ATM cards and personal identification numbers (PINs) were turned over to the organisers of the syndicate. Stolen and altered cheques were then deposited into many of the accounts.

Example 23: Prepaid international telephonic cards serve as a cover for money laundering

Two banks in a European country (Country C) reported a series of STRs related to unusual deposits of cash made by the director of a domestic limited company involved in the trade of prepaid international telephonic cards in Country C and an African country (Country D). The cash funds, credited at regular intervals of time also by means of manager's relatives, were periodically transferred to a small company registered in another country (Country E), which was supposed to be the seller of the mentioned telephonic cards.

From research carried out by the FIU in Country C, the Country E registered company seemed to be a shell company without any real economic activity. On this premise, in order to investigate further on the matter, the FIU contacted the FIU in Country E. Thanks to the co-operation between the two FIUs it has been disclosed that:

1. the competent authorities in Country E were already conducting an independent investigation of the Country E company for suspicious financial transactions .
2. the nature of shell company of the mentioned company could be confirmed
3. the Country D partner of the Country C company was under investigation by the Country E customs authority for narcotics trafficking.

At present all the documents related to the STR mentioned above are now under investigation by the national public prosecutor in Country C.

57. Bureaux de change continue to be a preferred mechanism for the conversion of cash proceeds. Although Belgium described a decrease in the number of STRs from bureaux de change in which narcotics proceeds were involved, there was an increase in the number of transactions dealing with trafficking of goods and merchandise (particularly as related to stolen cars and smuggling in alcohol and tobacco). Canada, Spain and Finland also reported either high or increasing reporting of STRs involving bureaux de change.

58. Value Added Tax (VAT) "carousel" fraud, a criminal activity specific to the European Union, was discussed in the typologies report for last year's exercise. This type of fraud works by means of a series of invoice manipulations that exploit the differences in VAT rates among the EU member countries and the exemption that allows businesses in one EU country to import goods legally from another EU member country without reporting the VAT. The over and under invoicing schemes used for VAT carousel fraud are very similar to techniques used in money laundering operations. There is a difference, however, in that the VAT carousel fraud is designed to avoid payment of VAT, whereas laundering through invoice manipulation is generally done in such a way that appropriate taxes and duties are paid at each step of the process (so as not to attract attention to the underlying laundering operation). Several FATF members reported that this type of fraud continues to occur and may in some cases be confused with laundering operations.

59. Traditional casino gambling has been confirmed as being a well used channel for money laundering in some FATF jurisdictions. Among others, Belgium made an observation in this respect on the basis of the implementation of a better detection method for this type of laundering since 1999, and Italy sees a certain amount of its traditional organised crime involved in such activity. The United States has detected the use of non-bank financial institutions in laundering operations involving gambling. In such schemes, funds are cashed out by the suspected launderer or moved to other accounts with little or no associated gaming activity. Other variations of this type of operation include cases where an initial deposit by wire or bank cheque are made. Then the funds are moved by wire to another account or stored temporarily in a safe deposit box at the casino before being cashed out.

60. Some of the money laundering techniques mentioned by the experts were characterised as relatively unsophisticated, such as currency smuggling or purchasing assets and property directly with criminal proceeds. Hong Kong, China, reported a scheme whereby launderers take advantage of the vicinity of three separate administrative regions[19] to move funds out of reach of the jurisdiction in which the funds were generated. This scheme was then combined with more complicated procedures using trade activities to repatriate the funds. In Italy, a recent scheme was uncovered in which a member of an organised crime group invested criminal proceeds directly into real estate purchases under the names of family members and other trusted persons in a vain attempt to avoid seizure under anti-mafia statutes.

61. The experts also discussed the use of leasing by launderers as a possible means of obtaining use of high value items (expensive cars, homes, etc.) without having to fear eventual loss to confiscation or seizure should their operations be discovered by authorities. It may also be used as directly for money laundering purposes. This practice was detected by accident when it was found in one jurisdiction that a leasing company had been receiving payments for the lease of a high-value car in cash which ultimately turned out to be the direct proceeds of criminal activity. In another case, a launderer paid a year's lease for a house in cash and then cancelled the lease the next day. The launderer received a reimbursement for the lease by means of a cheque from the leasing agency.

62. Investment in corporate vehicles is a technique cited by some of the experts as another means of laundering. In the US, there has been a noted increase in the use of shell or holding companies – that is, companies that engage in no apparent business activity and serve only as a conduit for funds or securities – in laundering operations. These formations have been indicated by STRs that reveal

[19] The Hong Kong and Macau Special Administrative Regions and the People's Republic of China.

complex activity, often involving foreign transactors in certain non-cooperative countries and territories. The complexity of the activity refers to the routing (originator, beneficiary, or intermediary institutions) and / or the lack of logic for the geographic extent of the scheme. Suspicious wire transfers totalling more than USD 500 million have been associated with such activity.

63. One FATF member has indicated that certain investment opportunities – specifically in endowment policies –may also have been used in money laundering. Endowment policies are typically long running investments linked to stock market performance, which pay out a lump sum after a number of years – usually 10, 15, or 25. The policy is usually supported by a monthly payment, although lump sum endowment policies are not unknown. Their potential use in money laundering concerns the secondary market in policies, which allows individuals to take over a policy (and upkeep costs) for an agreed price, with the eventual lump sum being paid to the new owner. In some cases the endowment policy records at the financial services provider will still show only the original owner, with the "new" purchaser only identified in management text.

64. As evidenced by US suspicious transaction reporting (and noted in last year's typologies exercise), there appears to be a continued trend in suspicious activity in which funds are wired to or through a US financial institution from a foreign source and then withdrawn in cash in a third country using ATMs. The STRs indicate such ATM withdrawals as taking place in several Latin American countries. The wire transfers that start the cycle originate primarily in Europe. Amounts up to several hundred thousand US dollars have been withdrawn using this method.

(iii) Counter-measures (new or modified)

65. Since the last FATF typologies exercise, a number of FATF jurisdictions have taken steps to upgrade or reinforce their anti-money laundering regimes. Following the passage last year of Japan's new anti-money laundering legislation, a financial intelligence unit (JAFIO) became operational in February 2000. Canada has enacted significant legislation as well, which makes suspicious transaction reporting mandatory, creates a cross-border reporting requirement for the transport of funds and establishes the basis for a financial intelligence unit (FIU). The Canadian FIU (FINTRAC) came into existence in July 2000 and will become fully operational in late 2001 when it begins to receive STRs.

66. In Hong Kong, China, amendments to the anti-money laundering ordinance extended money laundering preventive measures to the bureau de change and money remittance sector. The new provisions require that these businesses register with the Hong Kong Police. A failure to do could lead to criminal penalties. These businesses must also identify customers, maintain records and report suspicious transactions. The government is in the course of introducing amendments to the Drug Trafficking (Recovery of Proceeds) Ordinance and the Organised and Serious Crimes Ordinance to include an increased penalty for money laundering (from 14 to 20 years), creation of a new money laundering offence with lower mental element (maximum 5 year penalty), and facilitated restraint of property.

67. Denmark has extended its list of predicate offences for money laundering to passive and active bribery and fraud committed against the European Union, and it continues to consider moving to an "all serious crimes" money laundering offence. Spain has extended anti-money laundering obligations to notaries and to real estate and mercantile registries. In Sweden, legislation has been modified to bring money transmitters under similar anti-money laundering obligations to those to which bureaux de change and other non-bank financial institutions are subject. Germany appears to have cleared the way for creating a national financial intelligence unit with the establishment of a central database for STRs and a lowering of the restriction for its joint police and customs anti-money laundering unit to co-operate with foreign administrative type FIUs.

(iv) Information specific to FATF-style regional bodies

68. The money laundering methods and trends described in the previous section are not limited to FATF member countries. The FATF experts therefore devoted a portion of the typologies meeting to examining the money laundering situation in other areas of the world. The FATF-style regional bodies provided a great deal of material in the form of case studies and other information to support this effort. Despite a significant number of representatives from the regional bodies, however, the participating countries were still too few to provide a complete picture of each region of the world. The information that follows should therefore be seen as a partial overview of the money laundering situation in these regions.

a. The Americas

69. The CFATF is an FATF-style regional body with a membership made up of most of the countries of the Caribbean Basin. It holds regular typologies exercises of its own which usually focus on a single major money laundering issue. Recent work in this area has focused on free trade zones and their role in money laundering schemes, and an attempt was made to examine the connections between such locations and large scale alternative remittance systems, such as the "Black Market Peso Exchange"[20]. CFATF also is continuing its role of review of the anti-money laundering laws of its members to help ensure that they meet world-wide standards.

70. Until this year, the CFATF was the only FATF-style regional body within the Americas region. In December 2000, the countries of South America met in Cartagena, Colombia, to sign a memorandum of understanding that would bring the Financial Action Task Force for South America (GAFISUD[21]). GAFISUD's functions will be similar to the other regional bodies, that is, to assist and monitor its members' implementation of anti-money laundering laws and regulations.

71. Narcotics trafficking is the key source of funds laundered in many of the countries of this region; however, there is also a substantial amount of laundering that may be derived from other types of criminal activity. Some of the money laundering methods found in the region, according to the experts, include the structuring of cash deposits into financial institutions, the use of International Business Companies set up in certain jurisdictions, wire transfers, and alternative remittance systems. Cash proceeds play a significant role in certain stages of the money laundering schemes found in this region.

b. Africa and the Middle East

72. In previous years, up to date information for these two regions was difficult to obtain. With the establishment of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) and the just created Intergovernmental Task Force against Money Laundering in Africa (GIABA[22]), two new FATF-style regional bodies, more information about money laundering methods and trends in this area of the world is becoming available. Few of the jurisdictions have yet been able to implement comprehensive anti-money laundering laws, and many of factors are present that could be exploited for laundering purposes. Indeed, experts from the region and others familiar with it advised that there is an interconnection between Africa and the rest of the world with regard to money laundering by describing a few recent cases. In one apparent money laundering operation, high-value automobiles stolen in Japan found their way to Africa by way of the Middle East. In another scheme, wire transfers from a post office in Paris were sent to various villages in western Africa where the inhabitants are not even able to read.

---

[20] See *FATF-XI Report on Money Laundering Typologies, 1999-2000*, for a comparison between this system and other major alternative remittance systems.

[21] *Grupo de Acción Financiera de Sur America contra el Lavado de Activos*

[22] *Groupe intergouvernemental d'action contre le blanchiment de l'argent en Afrique*

73. According the ESAAMLG experts, a key element that might favour laundering in the region is the strong need for investment of capital from outside the region. Every investment dollar creates jobs; therefore, these countries are looking to attract as much investment as possible – even to the point of turning a blind eye to funds of questionable origin. There are many opportunities to invest in farms for tourism, for example. A lot of money can be placed in such operations, left there for a few years, and then taken away again with the sale of the property. Besides the need to establish anti-money laundering legal structures, there is also a need throughout most of Africa for technical assistance for investigators and additional resources to permit government authorities to verify the backgrounds of potential investors.

74. In western and central Africa, not only drugs but also corruption, various forms of fraud, and car theft are primary source of criminal funds that are laundered there. In addition to simply wiring the funds to other locations, laundering operations rely on alternative banking systems similar to the hawala and hundi system or on speculation operations involving commodities (coffee, for example). Some experts indicated that there continues to be laundering through alternative remittance systems between north-western Africa and south-western Europe as reported last year.

75. Information on laundering activity in the Middle East is very limited other than the few case examples that mention laundered funds or other assets transiting certain regional financial centres. It is hoped that, with the increasing awareness in this region of the problem of money laundering, more information on money laundering methods and trends will become available.

c. Asia / Pacific

76. Information on the money laundering methods and trends in the Asia / Pacific region continues to improve. The Asia/Pacific Group on money laundering continues to hold annual typologies exercises specifically focusing on that region. The last meeting was held in Bangkok, Thailand, in March 2000, and was devoted to underground banking and the use of false identities in money laundering. A report containing a compilation and analysis of cases dealing with the Asian alternative remittance systems[23] was presented and discussed at that meeting.

77. The primary sources of criminal proceeds include trafficking in narcotics and in human beings, gambling, corruption, and organised crime activities. Alternative remittance systems are a key method for moving funds. However, because of the reliance on cash as the principal means of payment, there is also a certain amount of cash smuggling, as well as various schemes to place funds in directly in the banking system. In other countries of the region, there have also been more complex laundering schemes involving use of criminal proceeds as collateral for loans or justifying their origin as the return of share deposit money.

d. Europe

78. Better information on the money laundering situation in non-members of FATF in Europe is becoming increasingly available perhaps due to the proximity of a large number of FATF members and the participation of both FATF and non-FATF countries in common European fora. The Central and Eastern European region continues to be cited as a significant source for what are believed to be criminal proceeds, as well as the criminals involved in what appear to be laundering schemes. Increasing co-operation between the financial intelligence units in FATF and non-FATF countries of the region is an important factor in better understanding the character and degree of the money laundering problem in Europe.

79. The Council of Europe PC-R-EV Committee continues both its work of evaluating the anti-money laundering systems of its 22 members and of conducting typologies studies. At the PC-R-EV

[23] Hawala and the Chinese / East Asian alternative remittance systems.

typologies meeting in February 2000, the Committee looked at the links between organised crime in the region and money laundering operations.

80. The most common predicate offence for money laundering among these countries is fraud (i.e., the looting of government holdings or financial institutions in former Communist Bloc countries). To a large extent, cash proceeds of crime are deposited directly into bank accounts and then withdrawn from other institutions. There are also laundering schemes that have used false invoicing or transfer pricing. Fly-by-night companies are a problem in some jurisdictions as an element of laundering and fraud schemes. The rise of multiple organised crime groups as related to narcotics trafficking means that the generated proceeds are distributed more widely, thus they are more difficult to detect for law enforcement. Bureaux de change are increasingly found in laundering operations, and there is some concern about suspected collusion between such businesses and organised crime.

IV. CONCLUSION

81. The year 2000 is now the fourth in which the FATF has focused discussions at its typologies meeting on a series of major money laundering issues. During the two-day meeting in Oslo, experts were invited to examine five areas of concern to law enforcement agents, regulatory officials and ultimately national policy makers. They were then asked to draw conclusions about these subjects that would also be included as part of their work.

82. The concerns raised during the FATF-XI typologies exercise regarding the possibility offered by the Internet for increased anonymity and geographic separation for a launderer – but without clear indicators of criminal use – led to another, broader examination of the subject this year. Further consideration of these factors has reinforced the perception that the areas of customer identification, know your customer policies and jurisdictional issues must be addressed again with the increasing usage of on-line banking. The role of the Internet itself, especially in respect to other web-based laundering schemes, also became clearer through this year's work. One key aspect for dealing with potential misuse of the system identified in this year's exercise is to focus on ensuring that connections can be traced using records that may be – and in many cases already are – maintained by the Internet computer servers. The rapid increase in Internet use means that development of appropriate policies cannot be delayed.

83. Despite their legitimate use and very long tradition in many jurisdictions, trusts, along with various forms of corporate entities, are increasingly perceived as an important element of large-scale or complex money laundering schemes. The FATF experts looked at this issue by briefly examining the nature of the trust as a legal relationship, its uses and the variety of its forms. It became clear from this examination that the concern for anti-money laundering authorities is the seemingly impenetrable anonymity which a trust may provide to the true owner or beneficiary. This anonymity is enhanced by the fact that documentation of trusts is not public information. Certain types of trust are more often misused than others (the blind or black hole trust and the asset protection trust) and may therefore warrant specific action to prohibit their use. Other possible solutions range from establishing a strict regulatory regime for trust formation agents (i.e., subject them to licensing, customer identification, record keeping and reporting requirements) to imposing some sort of public or semi-public registration requirement.

84. Lawyers, notaries, accountants and other non-financial professionals often play the role of "gatekeepers", that is, through their specialised expertise they are able to create the corporate vehicles, trusts, and other legal arrangements that facilitate money laundering. Professional confidentiality, which has traditionally applied to the relationship between the lawyer and the client for advocacy purposes, now is often extended to other non-advocacy "gatekeeper" functions. This makes the use of such professionals attractive to those individuals wishing to hide assets or launder money. One

solution is to encourage the inclusion of these professions under the same anti-money laundering obligations as financial intermediaries when they are performing similar functions.

85. Despite the increasing development of cashless payment systems such as the Internet, bank and wire transfers, etc., a significantly large portion of criminal proceeds is still generated in cash form. In some cases, certain criminal activities are more likely to produce cash proceeds, such as the drugs trade. Cash transactions remain the norm in many countries of the world. Laundering still takes place through the purchase of high-value or luxury items for cash (thoroughbred race horses, for example) or, in some cases, through the cash payment for services (leasing contracts). Some jurisdictions have actually reported increases in the number of STRs dealing with cash despite a decrease in the number of banknotes in circulation. Cash movements across borders is a growing phenomenon in some countries as launderers find it too difficult to place cash proceeds directly into the financial system. Nevertheless, some experts warned that overemphasising typologies involving criminal proceeds in cash form means that typologies for other forms of payment are not being developed, such as for wire or bank transfers. It appears therefore that, although a continued focus on cash as the weak point in the laundering process is still valid, it is nevertheless vital that work be undertaken to develop typologies for other forms of payment.

86. The FATF undertook this year to examine the ways that terrorist groups move or conceal funds in order to support their operations. One purpose of this examination was to see whether there were significant differences between the methods used by terrorists and those used by organised crime groups. Material obtained by the experts appears to indicate that there is little difference, first of all, in the source of funding for both types of groups: terrorists generate proceeds to support their activities through criminal activity (and sometimes from contributions or donations) in virtually the same way that organised crime does. The methods used for laundering funds in both cases are also virtually the same. A large number of countries also consider that terrorist acts or even affiliations with such groups constitute a serious crime. Where the difference occurs is in the counter-measures that may be applied in various jurisdictions. Some countries are not able to use anti-money laundering legislation for tracking or restraining suspected terrorist money if the source of the funds was voluntarily contributed and not a criminal act. There are also differences between jurisdictions as to which groups are classified as terrorist organisations. Certain of the FATF experts were of the opinion that terrorist related money laundering is a distinct sub-category of money laundering. Other experts held the opposite view and believe that terrorism can be adequately targeted under existing laws. This disagreement could not be resolved.

87. As in previous years, the FATF experts considered other money laundering methods and techniques beyond the five specialised topics. This exercise also attempted to look at trends outside the FATF membership by inviting representatives of the FATF-style regional bodies to participate. In many instances, previously identified laundering methods are now being found in new locations, or what appear to be new techniques – upon closer examination – turn out to be merely clever refinements of the old "tried and true" methods. Although this year's work appears to have revealed few truly new money laundering methods, the case examples and the material provided by the experts demonstrate the imagination and the tenacity of launderers in combining various techniques and mechanisms in order to legitimise criminal funds and to avoid detection. It also shows that, in spite of the differences among the anti-money laundering programmes of individual jurisdictions, all countries are faced with the similar problem of finding effective counter-measures. The better understanding of the characteristics, the evolution, and the world-wide reach of money laundering as derived from typologies analysis can only reinforce efforts to promote global anti-money laundering principles.