FAFT-VIII

FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING

ANNEXES OF THE ANNUAL REPORT 1996-1997

FAFTAX97.PM5

June 1997

ANNEX A

FATF-VIII REPORT ON MONEY LAUNDERING TYPOLOGIES

I. INTRODUCTION

1. The group of experts met in Paris on 19-20 November 1996 under the chairmanship of Mr. Stanley Morris, Director, Financial Crimes Enforcement Network (FinCEN). The group included representatives from the following FATF members: Australia, Austria, Belgium, Canada, Denmark, Finland, France, Germany, Ireland, Italy, Japan, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. Experts from non-member, observer organisations: Interpol, the International Organisation of Securities Commissions (IOSCO) and the Inter-American Drug Abuse Control Commission (OAS/CICAD) were present as well. In addition, representatives from the Organisation for Economic Co-operation and Development (OECD) attended some of the discussions on new technologies payments.

2. The purpose of the 1996/1997 "typologies exercise" was to provide a forum for law enforcement experts - those primarily tasked with combating money laundering - to discuss recent trends in the laundering of criminal proceeds, emerging threats, and effective countermeasures. While the discussions focused principally on money laundering developments in FATF member nations, the experts also sought to pool available information on prevailing money laundering patterns in non-member countries or regions.

3. A special topic of discussion for the 1996/1997 typologies exercise was the subject of current technologies developments in alternate payment methods - in particular payment systems using smart cards and the Internet. This subject was built into the 1996/1997 agenda to expand on the work begun in last year's typologies exercise, and to continue discussions which were commenced in the financial services forum of January 1996. To facilitate the dialogue, private sector representatives of organisations engaged in issuing or providing the new payment methods attended the meeting and gave presentations on more detailed aspects of their systems. In addition, representatives of a number of banking associations and other bodies interested in this topic attended the meeting.

4. The topics covered by the meeting were :

(a) monetary or percentage estimates of the money laundering that can be quantified, and if this was not possible, rough estimates of the size of money laundering activities relative to the amount of legitimate activities;

(b) the principal sources of illegal proceeds laundered;

(c) the principal money laundering methods detected in the following sectors : banking, non-bank institutions and non-financial businesses;

(d) electronic funds transfers and whether there are difficulties in identifying the ordering customer in an electronic funds transfer transaction;

(e) new (and/or proposed) money laundering counter-measures (legislative, regulatory, policy, etc.);

(f) non-FATF members - key money laundering centres/regions including details relevant to items (b) - (e) above.

II. ESTIMATE OF THE MONEY LAUNDERING PROBLEM

5. Due to the difficulties in deriving an accurate and precise figure for the amount of money laundering which is taking place in FATF members, it was agreed that as part of their submissions members would endeavour to provide some rough estimate of the amount of money laundering occurring in their countries.

6. Unfortunately, the vast majority of FATF members lack sufficient data to support any credible estimate. The most comprehensive figures remain the results of the study produced by the Australian delegation for 1995 which projected the amount of money laundered in that country to be approximately $3.5 billion (US$ 2.8 billion) during 1995.

7. Several members provided evidence of the number of suspicious transaction reports filed in their countries and the amounts involved in those transactions. These figures ranged from US$ 45 million in one country to US$ 800 million in another. However it was recognised that this figure is clearly a subset of the total amount of money laundering.

8. Other experts offered data on sums seized pursuant to money laundering investigations or prosecutions. Thus one member was unable to establish the magnitude of money laundering taking place, but as an example could show that one law enforcement agency for the partial year (1 October 1995 - 31 August 1996), had 1,233 cases of money laundering prosecuted with a total value of US$ 1.62 billion. However this information too does not support a valid estimate of the amount of tainted funds entering the legitimate financial stream, as it is can only be a small percentage of the total amount of proceeds of crime.

9. The considerable difficulties in calculating the size of the money laundering problem were recognised by the experts, and there were differing opinions as to the practicality of continuing attempts to estimate. Whilst a statistically significant estimate would provide valuable information, the lack of available statistics, and the difficulties with methodology could make such a study a very difficult and time consuming exercise. Other experts suggested that an accurate estimate would be an important tool to measure whether anti-money laundering measures were having any effect, and would provide important information for governments. A more modest objective for the short term was suggested - namely the compilation of accurate and comprehensive statistics on matters such as money laundering convictions, seizures, and confiscation. One international organisation noted that the number of money laundering cases reported to it had increased from 215 in 1992 to about 900 in 1996. Other experts noted that such statistics are often misleading, and do not give an accurate picture of the size of the problem.

III. RECENT TRENDS AMONG FATF MEMBERS

A. <u>The Principle Sources of Illegal Proceeds</u>

10. Drug trafficking and financial crimes (bank fraud, credit card fraud, investment fraud, advance fee fraud, bankruptcy fraud, embezzlement and the like) remain the most frequently mentioned sources of

illegal proceeds. As in the 1995/96 report, drug trafficking is still the largest single generator of illegal proceeds, but the amount of laundering linked to financial crime is also very significant and the Scandinavian members continued to report greater levels of illicit profits stemming from financial crimes than from narcotics. A number of countries also indicated that smuggling of goods (often items that were highly taxed such as alcohol or tobacco) generated a very large amount of proceeds which was being laundered.

11. Criminal activity which is linked to organised crime also continues to be responsible for a large proportion of the dirty money flowing through financial channels. Organised crime groups in Italy, Japan, Colombia, Russia and Eastern Europe, Nigeria and the Far East, and other similar groups are involved in a wide range of criminal activities. In addition to drug trafficking, these enterprises generate funds from loan sharking, illegal gambling, fraud, embezzlement, extortion, prostitution, corruption, illegal trafficking in arms and human beings, organised motor vehicle theft and many other offences. A trend was also noticed in some countries whereby criminals who had been solely engaged in drug trafficking were either broadening their activities to take part in a wider range of criminality, or had switched to fraud and other offences which attracted lower penalties.

12. Many European countries continued to find that significant amounts of cash and other forms of payment were flowing into their countries from the former Soviet Union and other Eastern Europe countries. There remain major difficulties in many cases in identifying whether this money is the proceeds of crime or capital flight money, and if identified as having an illegal origin, it is remains very difficult to determine what the predicate offence was. Although co-operation had been received from the law enforcement authorities in certain Eastern European countries in some cases, this was not consistent, and on many occasions investigations were not completed due to an inability to identify the predicate offence.

B. Current Trends in Money Laundering

13. Some general observations can be made regarding the methods of money laundering currently in use in the FATF members. First, no significant new methods of money laundering were identified by member states, and indeed a number of traditional money laundering techniques continued to be prominent methods for hiding the proceeds of crime. Second, although there were no new methods, there continues to be changes in the relative use of the various money laundering methods, and in particular there was a continuing trend for money launderers to move away from the banking to the non-bank financial institution sector.

14. Almost all members felt that there was a continuing increase in the amount of criminal cash being smuggled out of their respective countries for placement into the financial system abroad. In many European countries there are no cross border controls on the movement of cash, and it is relatively simple for launderers to take large sums of cash by road to neighbouring countries. As with drugs, the authorities believe that whilst large amounts of cash are carried on the passengers person, an even greater amount may be hidden in cargo or goods shipments. The continuing trend of cash smuggling appears to be mostly attributable to the success of anti-money laundering measures in banks and other financial institutions. A corresponding feature of cash smuggling is the detection of a significant amount of cash stockpiling.

15. An interesting trend in one country appears to be that money laundering cells try to limit the amount in any single accumulations of funds to US$ 300,000 to US$ 500,000. The reason for this appears to be to limit losses due to seizure by law enforcement or theft. Although this limit seems to

apply to any method of money laundering (smurfing, wire transfer, etc.), it is especially apparent in currency smuggling.

(i) The Banking Sector

16. Banks remain an important mechanism for the disposal of criminal proceeds, though there appears to be a recognition by money launderers that obvious techniques such as depositing large sums of cash into bank accounts for subsequent transfer is likely to be reported to law enforcement authorities, and thus extra steps are being taken. A significant number of countries reported that the technique of "smurfing" or structuring was commonly used - this technique entails making numerous deposits of small amounts below a reporting threshold, usually to a large number of accounts. The money is then frequently transferred to another account, often in another country. This method was widely used, even in countries which did not have cash transaction reporting requirements, which require reports to be made to the authorities of transactions above certain thresholds. Countries to which these funds were transferred often found the funds being promptly removed as cash from the recipient accounts. In one member, it was found that increased awareness of this technique was causing smurfers to deposit smaller sums e.g. US$ 2,000-3,000, into more accounts, so as to try to avoid detection.

17. Perhaps because of improved customer identification requirements there appears to be less use of accounts in false names. However there continues to be many instances of the use of accounts held in the name of relatives, associates or other persons operating on behalf of the criminal. Other methods commonly used to hide the beneficial owner of the property include the use of shell companies, almost always incorporated in another jurisdiction, and lawyers. These techniques are often combined with many layers of transactions and the use of multiple accounts - thus making any attempts to follow the audit trail more difficult.

18. The shell corporation is a tool which appears to be widely used in almost all members in both the banking and non-banking sectors. Often purchased "off the shelf" from lawyers, accountants or secretarial companies it remains a convenient vehicle to launder money. It conceals the identity of the beneficial owner of the funds, the company records are often more difficult for law enforcement to access because they are offshore or held by professionals who claim secrecy, and the professionals who run the company act on instructions remotely and anonymously. These companies are used at the placement stage to receive deposits of cash which are then often sent to another country, or at the integration stage to purchase real estate. They have also been the vehicle for the actual predicate offence of bankruptcy fraud on many occasions.

19. Another technique which appears to be widely used, particularly by ethnic groups from Africa or Asia, is the "collection account". Immigrants from foreign countries would pay many small amounts into one account, and the money would then be sent abroad. Often the foreign account would receive payments from a number of apparently unconnected accounts in the source country. Whilst this payment method is certainly used for legitimate purposes by foreign immigrants and labourers who send money to their home country, this fact has been recognised by criminal groups who use this method to launder their illegitimate wealth.

20. Some delegations noticed attempts by organised crime to infiltrate smaller banks and non-bank financial institutions, or even that criminal organisations in certain regions of the country sought to extend this control to a large range of businesses in that area. Experts from several member countries uncovered money laundering schemes involving complicit bank directors or employees, and in one member a noticeable trend was the assistance provided by "private banking representatives" (bank employees who provide special services to wealthy customers) to "smurfs" who recycle the bank accounts used for

structuring purposes. They typically begin using an account by making deposits and withdrawals heavily. Then a few months before the bank audits those accounts, they stop the activity and leave a few thousand dollars in the account. The account will then show up in the audit as an account that has not had a great deal of activity in the last three months, and is thus less suspicious.

21. The use of "payable through accounts" by international money launderers, a trend reported by a member last year, persists. These are demand deposit accounts maintained at financial institutions by foreign banks or corporations. The foreign bank funnels all of the deposits and cheques of its customers (usually individuals or businesses located outside of the country) into one account that the foreign bank holds at the local bank. The foreign customers have signatory authority for the account as sub-account holders and can conduct normal international banking activities. The payable through accounts pose a challenge to "know your customer" policies and suspicious activity reporting guidelines. It appears that many banks offering these types of accounts have been unable to verify or provide any information on many of the customers using these accounts, which poses significant money laundering threats.

22. Loan back arrangements was also a technique used in a number of countries, often in conjunction with cash smuggling. By this technique, the launderer usually transfers the illegal proceeds to another country, and then deposits the proceeds as a security or guarantee for a bank loan, which is then sent back to the original country. This method not only gives the laundered money the appearance of a genuine loan, but often provides tax advantages.

23. In addition to the typologies outlined above, other familiar laundering techniques continue to figure prominently in the banking sector. Telegraphic transfers remain a primary tool at all stages of the laundering process because of the speed with which the money is transferred, thus making it difficult for law enforcement to trace illegal proceeds, particularly in several jurisdictions. Bank drafts, money orders and cashier's cheques also remain as common instruments used for laundering purposes. Large cash deposits are still being made in some areas, especially by persons and interests connected to the former Soviet Union and Eastern Europe, although drug traffickers still made significant cash deposits. Often the cash deposit was quickly followed by a telegraphic transfer to another jurisdiction, thus lowering the risk of seizure.

24. Members were asked if they had difficulties in identifying the ordering customer in electronic funds transfer transactions. Several countries indicated they had a problem with customer identification in this area. This was a problem for funds originating in offshore jurisdictions, or was associated with "payment through accounts". Another country had done a study which showed that lack of customer identification information on the telegraphic transfer message was a significant problem, and that up to 25% of messages from some jurisdictions did not have the ordering customer information that was needed. It was also noted that although sufficient information was received, the accuracy of some of the information recorded on the transfer message, particularly for funds that were transferred from the former Soviet Union and Eastern European countries, may be questionable.

(ii) Non-Bank Financial Institutions

25. Banks offer a wide range of financial products and hold the largest share of the financial market, and accordingly the services they provide are widely used for money laundering. However, non-bank financial institutions and non-financial businesses are becoming more attractive avenues for introducing ill-gotten gains into regular financial channels as the anti-money laundering regulations in the banking sector become increasing effective. Some delegations continue to report a significant shift in laundering activity from the traditional banking sector to the non-bank financial sector and to non-financial

businesses and professions. This is evidenced by the increasing numbers of suspicious transaction reports filed by such institutions (although this increase is also due to better compliance by such institutions), and the number of money laundering cases in which they are involved, relative to similar statistics for banks.

26. As reported last year, bureaux de change, exchange offices or casa de cambio pose an ever more significant money laundering threat. Almost all delegations reported a significant increase in the number of actual or suspected money laundering cases involving this type of institution. They offer a range of services which are attractive to criminals : (a) exchange services which can be used to buy or sell foreign currencies, as well as consolidating small denomination bank notes into larger ones, (b) exchanging financial instruments such as travellers cheques, Euro cheques, money orders and personal cheques, and (c) telegraphic transfer facilities. The criminal element continues to be attracted to bureaux de change because they are not as heavily regulated as traditional financial institutions or not regulated at all. Even when regulated the bureaux often have inadequate education and internal control systems to guard against money laundering. This weakness is compounded by the fact that most of their customers are occasional, which makes it more difficult for them to "know their customer", and thus makes them more vulnerable.

27. Remittance services (sometimes referred to as giro houses) have also proven to be widely used for money laundering, since they are often subject to fewer regulatory requirements than institutions such as banks which offer an equivalent service. They are also popular with many ethnic groups as they charge a lower commission rate than banks for transferring money to another country, and have a long history of being used to transfer money between countries. They operate in a variety of ways, but most commonly the business receives cash which it transfers through the banking system to another account held by an associated company in the foreign jurisdiction, where the money can be made available to the ultimate recipient. It was reported that another technique commonly used by money remitters and currency exchanges was for the broker to make the funds available to the criminal organisation at the destination country in the local currency. The launderer/broker then sells the criminal dollars to foreign businessmen desiring to make legitimate purchases of goods for export. This correspondent type operation resembles certain aspects of "underground remittance services".

28. Several members reported significant use of hawala, hundi or so called "underground banking", as well as other systems. This system is almost always associated with ethnic groups from Africa or Asia, and commonly involves the transfer of value between countries, but outside the legitimate banking system. The "broker", which may be set up as a financial institution such a remittance company, or may be an ordinary shop selling goods, has an arrangement with a correspondent business in the other country. The two businesses have customers that want funds in the other country, and after taking their commission, the two brokers will match the amounts wanted by their customers and balance their books by transferring an amount between them for the time period e.g. once a month. The details of the customers who will receive the funds, which are usually minimal, are faxed between the brokers, and the customers obtain their funds from the brokers at each end of the transactions. The experts agreed that it is difficult to determine the extent to which this alternative remittance service is used for money laundering, as the service is widely used for legitimate transactions, and because minimal records are kept. Indeed it is difficult to even identify the businesses which offer this service.

29. A number of experts also noted the use of single premium insurance products, and the early encashment of such policies. A limited number of cases of laundering of illegal funds in the securities sector were also cited. Some experts noted the potential future threat associated with the changeover to a single currency - the Euro - in Europe which is planned for 2002. Concerns were expressed that the change from national currencies to the Euro may offer significant opportunities for money launderers unless appropriate safeguards were introduced.

(iii) Non-financial businesses or professions

30. As anti-money laundering regulations have increased in many countries the criminals place increasing reliance on professional money laundering facilitators. The experts reported a significant number of cases involving lawyers, accountants, financial advisors, notaries, secretarial companies and other fiduciaries whose services are employed to assist in the disposal of criminal profits. Among the most common tactics observed have been the use of solicitors' or attorneys' client accounts for the placement and layering of funds. By this method the launderer hopes to obtain the advantage of anonymity, through the solicitor-client privilege. The making available of bank accounts and the provision of professional advice and services as to how and where to launder criminal money is likely to increase as counter measures become more effective.

31. In addition to the use of shell companies, there was also widespread use of real businesses, either to camouflage the illegitimate laundering of money or as part of the predicate offence, and the use of real businesses was more prevalent in relation to fraud and other financial crime than for drug offences. Techniques used in conjunction with these businesses included false invoicing, commingling of legal and illegal moneys, the use of loan back arrangements and layers of transactions through offshore shell companies. Often the laundered proceeds would then be invested through the real company into real estate or other businesses, though one country reported that there was a trend away from investing illegal proceeds in real estate, and into less visible investments such as financial businesses.

32. Casinos and other businesses associated with gambling, such as bookmaking, continue to be associated with money laundering, since they provide a ready made excuse for recently acquired wealth with no apparent legitimate source. The services offered by casinos will vary depending on the jurisdiction in which they are located, however the industry overall appears to recognise the threats from money laundering and is taking steps to minimise the risks by identifying its customers, looking for those persons who do not actually gamble etc.

33. A number of other money laundering techniques in the non-bank sector remain prominent. Substantial amounts of illegal proceeds are still invested in real estate. Interests in the former Soviet Union and Eastern Europe were found to invest in countries close to this part of the world, as well as in the Mediterranean region. Other techniques cited were the purchase and cross border delivery of precious metals such as gold and silver, and the use of financial instruments such as warrants in the metals market to transfer value between countries. This latter method was particularly associated with criminal organisations from Eastern Europe.

C. Developments in Counter-Measures

34. Almost all FATF members have implemented a significant number, if not all, of the FATF Recommendations. Some members made significant changes or additions to their basic anti-money laundering framework, whilst others have made refinements in light of the changing nature of the threat they face. The following are some of the more noteworthy developments which have been already completed or are planned.

35. Major initiatives were passed by New Zealand and Turkey during the year. New Zealand passed legislation to require reporting of suspicious transactions, customer identification and record keeping, whilst Turkey passed a Bill which created a money laundering offence which applies to a wide range of predicate offences as well as certain administrative matters.

36. Almost all members (23) have now taken action to extend the scope of their money laundering offence to non-drug related crimes. This trend is continuing in response to the evidence regarding the significance of non-drug related crime as a source of illegal wealth. France, Norway and Spain passed bills to criminalise money laundering in connection with all serious crimes, whilst Canada is considering do so. Portugal included terrorism, financial crimes, corruption, extortion and other serious crimes as predicate offences for money laundering, and Germany is considering adding further offences to its predicates. In addition, members such as Austria, Denmark, Germany, Hong Kong, Ireland and Norway have enacted or are considering legislation to make it easier to seize or confiscate the proceeds of crime - which often involves consideration of whether to reverse the burden of proof.

37. Members are also continuing to extend the reach of money laundering prevention measures to additional groups of businesses and institutions, particularly non-bank financial institutions. Four countries have enacted or are in the process of enacting legislation bringing bureaux de change under their anti-money laundering regimes. Norway has also extended its reporting requirements to the securities and insurance industries, as well as the Central Bank. Members are also focusing their attention on non-financial businesses which may be brought within the scope of the anti-money laundering framework. These include lawyers (Australia and Belgium), real estate agents and casinos (Belgium, Finland and Portugal), and notaries, auditors, pawnshops and bullion dealers.

38. Several members are changing the administrative structures governing the receipt of suspicious transaction reports by centralised financial information units (FIU). Five countries have or are establishing an FIU to receive, analyse and disseminate all such reports. Another country has continued with its monitoring of a program whereby financial institutions can use computerised systems for detecting suspicious transactions. Based on the results to date, they believe that this has been very successful. Many members were also making efforts to improve international co-operation at both the intelligence and investigation levels, and the experts said that the ability to obtain speedy and comprehensive assistance from other countries, particularly non-FATF members, needs to be further promoted.

IV. THE SITUATION IN NON-FATF COUNTRIES

39. Money laundering is not a problem restricted to FATF members, and indeed, as FATF countries take measures to combat money laundering it is likely that more money will be laundered through countries which have less well developed anti-money laundering standards. Information on the money laundering situations in non-FATF members is less developed, and for some parts of the world the experts had little information to report regarding money laundering trends or developments.

(i) Asia

40. The Asian region is characterised by several important features which affect the money laundering methods used in the region. First, the existence of the major drug production centres in the Golden Crescent (Afghanistan, Iran) and the Golden Triangle (Burma/Myanmar, Thailand, Laos). Secondly, the high level of use, for both legitimate and illegitimate transactions, of alternative remittance systems such as “hawala” or “hundi” system. Thirdly, the high use of cash, and the willingness to conduct large cash transactions. Finally, the existence of Chinese and Japanese organised crime groups which operate internationally and in the region.

41. The FATF Asia Secretariat and Interpol sponsored a meeting on money laundering in November 1996, and a brief summary of the meeting was given. This exercise and other information from FATF

countries revealed that the sources of illegal proceeds had not changed significantly. Drugs proceeds amounted to the largest part of the illegal money being laundered, with recent increases in the production of methamphetamines adding to the traditional proceeds of heroin trafficking. Large amounts of money were also being made from organised crime, arms smuggling, and the organised movement of illegal immigrants. In the South Asia region, gold smuggling and corruption provided further sources of illegal proceeds for laundering.

42. No new money laundering methods were noted, and generally the trends in Asia appear to be similar to those in FATF members. Several countries observed an increase in the amount of cross border smuggling of cash and bearer instruments such as money orders or bank drafts. Both telegraphic transfers and alternative remittance services were widely used, as were the use of false name or third party accounts at financial institutions. Other methods included the use of professionals such as lawyers, casinos, and false invoices and letters of credit. Illegal proceeds continued to be invested in high value items such as real estate.

43. The non-FATF countries in the region are at varying stage of development in terms of anti-money laundering legislation and measures, and several countries have passed new counter-measures. In 1995, Pakistan prepared a bill to criminalise drug related money laundering and impose certain reporting requirements on banks and financial institutions in Pakistan. Taiwan passed certain measures to combat money laundering in October 1996, whilst China has established a deadline of mid-March 1997 for the drafting of anti-money laundering legislation which is expected to be passed by the Peoples Congress later that month.

(ii) Central America, South America and the Caribbean Basin

44. According to one FATF member, money laundering has increased in the Western Hemisphere over the past year. This is attributed to increased drug trafficking, which is the main source of money being laundered, as well as various criminal activities carried out by organised crime groups, and an increase in smuggling.

45. The Caribbean Basin serves as an important transit point for drugs originating in Latin America bound for the United States, and is also the location for many offshore banks and financial institutions. Even when anti-money laundering legislation is enacted, other features such as liberal laws regarding company formation and the conduct of business activities in free zones make this region attractive to money launderers. There are many tens of thousands of shell companies incorporated in the region, whilst the number of free zones is increasing. The result is that the limited resources of regulatory authorities cannot effectively monitor the business activity which is taking place.

46. A trend has also been observed whereby Russian organised crime is seeking to launder profits from extortion, prostitution, arms sales and intellectual property theft in the Caribbean, and have relied on exploiting banking regulations in the region. Intelligence also suggests that the Russians crime groups may be forming alliances with other criminal groups operating in the region such as the Italian Mafia and Colombian cartels. These developments create considerable risks for the integrity of the banking system in the region.

47. A range of methods have been observed being used by Colombian drug cartels : (a) cartel intermediaries pay American exporters for goods exported to Columbia with drug dollars, whilst the importers pay intermediaries a slightly lesser amount in Colombian pesos, (b) a cartel money broker pays the exporter in a Free Trade Zone with drug dollars, the importer gives pesos to the broker and gets his merchandise, and the drug trafficker gets pesos to invest locally or fund drug operations. This is made

easier by the Free Trade Zones, which provide for the free movement of goods and cash with minimal government scrutiny, (c) the use of false import/export declarations and trade-related schemes, and (d) the structuring of cash transactions continues to be the primary technique used to penetrate the financial system, usually with the co-operation of corrupt bank employees.

48. In one Free Zone bank secrecy protects corporations and trusts, and the lack of customs enforcement controls does not allow for effective enforcement of laws requiring reporting of cash over US$ 10,000 being brought into the Zone. Launderers can purchase goods in the Free Zone and then sell it in cash transactions at 70% to 80% of face value to free port merchants thus avoiding customs and other regulations. They then deposit their pesos in banks located in the port, and transfer the money to false name accounts in their country. In the Free Zone it is also common to launder proceeds through third party cheques. Banks have also been bought and controlled by the Colombian cartels, who smuggle cash and cheques to deposit in the banks.

49. A major problem is the cross-border laundering of funds between Mexico and the United States This can take place by the smuggling of currency out of the United States, the use of payable through accounts that enable a person abroad to write a check at his or her own bank that is payable through the account of a correspondent United States bank, and cross-border telegraphic transfers. Mexican bank drafts (a draft which is drawn on an account with a United States bank that is held by the Mexican bank) are widely used to repatriate laundered funds to the United States as they do not have to be declared in the United States. Casa de cambio (exchange houses) along the border are also used in many money laundering operations since they exchange currency and perform wire transfers, and can thus intermingle illicit funds with legitimate exchange business.

50. Despite the range and extent of money laundering in the region, it was reported that progress is being made to implement the necessary measures. An important initiative in combating international money laundering was the Summit of Americas Ministerial Conference in December 1995, attended by 34 countries. The participating countries agreed to implement a range of measures : (a) enacting legislation to criminalise money laundering from all serious crimes; (b) expanding the mechanisms available to police authorities in investigating money laundering; (c) reviewing laws and regulations regarding bank secrecy to determine the extent to which these laws permit disclosure of financial institutions' records to competent authorities; (d) establishing programs for reporting suspicious or unusual transactions; (e) sharing information among countries for the investigation and prosecution of money laundering crimes and potential direct exchange of financial information between countries; and (f) the establishment of financial intelligence units to collect and analyse financial disclosures information.

(iii) Middle East and Africa

51. Limited information exists on this region although it is clear that there are considerable differences in the problems faced by the countries in the region. In the Arabian Gulf the problems cited most often are the hawala "banking" system and the use of the large gold market to launder funds. In the rest of the Middle East the most identifiable threat relates to Russian organised crime, which according to several reports is attempting to launder money in the region. Another potential threat is the diamond industry since diamonds - like gold - offer a portable store of value which is easily hidden.

52. Only a handful of countries in the area are in the process of taking anti-money measures. In April 1996 Cyprus passed a new, comprehensive anti-money laundering Act which expanded the list of crimes whose proceeds are subject to seizure or confiscation and provides for the establishment of a financial intelligence unit . The Israeli government in March 1996 drafted a law which would criminalise

money laundering for all serious crimes and would, in addition, allow for the establishment of a reporting system for suspicious transactions. However, the legislation has not yet been enacted and it is not clear when it will be reintroduced to the parliament. Lebanon has proposed legislation which would criminalise money laundering, but the law has not yet been submitted to Parliament, and in the Gulf some measures in relation to customer identification, record keeping and suspicious transaction reporting have been taken in relation to financial institutions. Apart from this little appears to have been done.

53. In Southern and Eastern Africa it was noted that there had been increases in fraud and corruption, and that narcotics trafficking, arms smuggling, theft and resale of commodities, and other white collar crimes generated considerable proceeds which were being laundered. Common methods of money laundering include purchase and resale of commodities, currency smuggling, purchase of real estate such as casinos and luxury hotels, and the establishment of privately owned banks. Use is also made of bureaux de change, which are largely unregulated throughout the region. In Southern Africa the gold and diamond industries and the hawala "banking" systems provide further risks, and in West Africa there is continued evidence of the involvement of Nigerian organised crime in international drug trafficking and large scale fraud.

54. Most countries in the region have not made money laundering a criminal offence nor do they have other anti-money laundering measures in place. Those that do tend to be restricted to drug money laundering, though countries such as Zimbabwe, Tanzania and South Africa (which has already enacted several important pieces of legislation) are further advanced. An encouraging development though was the holding of a Southern and Eastern African Money Laundering Conference in October 1996, jointly sponsored by the Commonwealth Secretariat and the FATF. Most of the countries in the region attended, and expressed a willingness to develop a unified approach to dealing with anti-money laundering issues in the region. The most notable result was the adoption of a proposal, subject to confirmation by heads of government, to establish a Southern and Eastern African FATF.

(iv) Eastern Europe and the former Soviet Union

55. Once again, criminals groups in Eastern Europe and the states of the former Soviet Union were cited in money laundering examples given by many FATF members . Large volumes of cash and other types of transfers continue to make their way from these countries into the banks and financial institutions of FATF member countries. Although a significant number of cases showed Russian organised crime groups and other illegal enterprises were using legitimate financial channels to launder ill-gotten wealth, it was not possible in many cases to confirm the origin of the funds in question.

56. The sources of illegal proceeds are for the most part generated within the region and can be categorised into four broad areas: (a) the illegal sale of natural resources such as oil, natural gas, metals, etc.; (b) the smuggling of alcohol, tobacco, arms, and drugs; (c) proceeds from traditional organised crime activity such as extortion, prostitution, theft, fraud, motor vehicle theft, etc.; and (d) white collar crimes such as the embezzlement of state property and funds, income and profit declaration evasion, tax fraud, tax evasion, and illegal capital flight. Foreign sources of illegal proceeds entering the former Soviet Union to be laundered have not been well documented.

57. The most commonly cited method of laundering in the region continued to be cases in which individuals opened accounts at financial institutions and deposited large amounts of cash tied to interests in the former Soviet Union and Eastern Europe. Once deposited, the funds were then transferred out of the country. Often these schemes involved the assistance of a lawyer or other professional. Offshore shell companies and trading or other front companies were also commonly used to receive fund transfers and then transfer the money on elsewhere.

58. Other common methods used to launder assets are false invoicing schemes, keeping of a double set of books, and contract fraud. A common scenario is a wire transfer of funds in foreign currency to a front company abroad for a commercial transaction. A fraudulent purchase contract provided by the front company is presented to the bank as proof of the commercial need for wiring the funds. After the funds are wired, the legitimised funds are free to be transferred or converted to cash. This method is also used to embezzle state funds.

59. The types of financial institutions and non-financial businesses used to launder proceeds include banks, currency exchanges and other non-bank financial institutions, casinos, and real estate companies. Banks are commonly used to launder funds from domestic and foreign sources, and although bank drafts and travellers checks have been generally used to launder proceeds, the majority of transactions are conducted either in cash or through telegraphic transfers.

60. Groups tied to the former Soviet Union and Eastern Europe are continuing to make extensive investments in real estate, hotels, restaurants or other businesses in a number of Western European countries. The assets are often purchased through offshore companies with the assistance of an intermediary. Some delegations also noted links between Russian organised crime and other similar groups such as the Mafia.

61. Money laundering countermeasures are in varying stages of adoption and implementation. Russia passed a law criminalising the laundering of a wide range of offences which came into force on 1 January 1997, and has an anti-money laundering Bill before the Duma containing measures for the financial sector and related administrative matters. Measures in the Baltic States are at early stage of development, although Lithuania has a number of basic provisions in place. With respect to the other nations of the former Soviet Union however, only Belarus appears to be in the process of drafting anti-money laundering legislation. Countries in Eastern Europe are further advanced, and some have developed more comprehensive anti-money laundering systems.

V. DEVELOPMENTS IN NEW TECHNOLOGIES

62. All the major providers and issuers of e-money were invited to the meeting, and four organisations which were representative of the different types of systems currently available, gave an overview of their systems. In addition to FATF members and observers, a number of banking associations e.g. International Banking Security Association and the Banking Federation of the European Union, and international organisations such as the Organisation for Economic Co-operation and Development (OECD) and the Bank for International Settlements (BIS) were present and contributed to discussions. The four presenters were:

- SIBS: The Sociedade Interbancaria de Servicos (SIBS) is Portugal's leading bank payments company. In addition to its Automated Teller Machine and Point of Sale networks, SIBS has introduced the Multibanco Electronic Purse;

- Mondex: Mondex International, which is based in the United Kingdom, is the provider of a stored value card that allows transactions between individuals and merchants as well as between individuals;

- Cybercash: Cybercash is an Internet-based system based in the United States. Recently, Cybercash announced that it was working with Mondex to develop a hybrid system in which stored value cards could be used in connection with Cybercash's software;

- Interpay: Interpay is based in the Netherlands and is the payment processing organisation for all Dutch banks. Interpay has introduced the ChipKnip which is an Internet-based system that allows the purchase of tokens to buy goods.

63. Based on these presentations and the material previously made available the current or developing systems can be divided into three categories : stored value cards, Internet/network based systems, and hybrid systems which are interoperable between the former systems. After the presentations, a broad discussion was entered into concerning the issues raised by law enforcement with respect to money laundering, particularly the effectiveness of existing regulatory policies and law enforcement techniques, and international jurisdictional issues.

64. There is no single design feature of the various e-money systems currently available or envisaged which will make them especially attractive to money launderers. Important features of these systems which will affect the degree to which they can be used by criminals are :

- the value limits placed on cards and Internet accounts/transactions;
- to what degree stored value cards will become interoperable with Internet based systems;
- whether stored value cards will be able to transfer value between individuals rather than just to or from a merchant;
- whether there will remain any intermediaries in these new payment systems; and
- whether account opening and/or transaction records will be kept, and in what detail.

65. The primary law enforcement issues that emerged were: (a) the need to review and potentially revise existing regulatory regimes to ensure adequate supervision of all types of e-money providers; (b) whether accurate and adequate records of the transactions and persons involved will be available; (c) stored value cards may be more difficult to detect than physical currency; and (d) the speed and volume of e-money transactions may make it more difficult to track or identify unusual patterns of financial transactions.

66. For those e-money systems are being designed to operate internationally and in multiple currencies, another challenge facing law enforcement will be the difficulty in determining jurisdictional authority. The current regulatory and law enforcement framework relies on defined financial and geographic borders. The diminishing of international financial borders makes it even more necessary to enhance cooperation and coordinate efforts among nations to ensure that there are consistent policies and standards.

67. However, it was agreed that the application of new technologies to electronic payment systems is still in its infancy, and that how these systems develop will depend on a combination of the effectiveness and efficiency of these technologies, the market and consumer acceptance. Therefore, it is premature to consider prescriptive solutions to theoretical problems. However, it is important for law enforcement and regulators to continue to work to understand the issues that need to be considered and perhaps addressed as markets and technologies mature.

68. The e-money industry representatives stated that they want and need more feedback from law enforcement in order to understand their concerns and to be able to incorporate possible solutions into their systems, and law enforcement must continue to reach out to the industry to increase its knowledge about the operations of such systems. For example, measures that are necessary for anti-money laundering purposes need to be considered alongside the safeguards that the industry is building in to prevent fraud and other security issues. Continued discussion on the issues mentioned above and on other

topics such as the right to privacy and cost effectiveness are a necessary part of future co-operation between the financial services industry, the FATF, law enforcement and regulatory experts.

69. It was clear that there are many similar efforts underway with respect to e-money and that FATF should continue its partnership with the industry and other international organisations to coordinate and facilitate communication. The Annex to this paper contains a more detailed description of the discussion.

VI. CONCLUSIONS

70. Money laundering remains a very serious problem in FATF countries and around the world. Laundering is a necessity for any profit-generating criminal activity, and narcotics traffickers, perpetrators of financial fraud, organised crime groups and others invest considerable effort into laundering their illicit proceeds, so that they can eventually live a expensive lifestyle from it.

71. It remains difficult to assess the scale of the money laundering problem. There is general agreement that it amounts to hundreds of billions of dollars annually, but that attempts to arrive at a precise estimate will require a comprehensive study. This may be difficult given that a number of members were unable to offer even a rough estimate of the amount of money being laundered in their country. Given the difficulties and the resource implications, opinion was divided as to the merits of proceeding with the comprehensive and methodologically sound study which would be required.

72. In most members, drug trafficking remains the single largest source of illegal proceeds, although the experts agreed that non-drug related crime is increasingly significant The other major source of proceeds were from various types of fraud, smuggling, and offences connected with organised crime. Indeed, it appears that there is a trend in some countries for career criminals and organised crime to switch from drug trafficking to non-drug crime because of the lesser penalties which apply to these types of offences. Drug traffickers are also engaging in a range of other offences, with funds being laundered and commingled from several forms of criminality.

73. As regards money laundering techniques, the most noticeable trend is the continuing increase in the use by money launderers of non-bank financial institutions and non-financial businesses relative to banking institutions. This is believed to reflect the increased level of compliance by banks with anti-money laundering measures. Traditional methods remain most popular, as is demonstrated by the increase in cash smuggling across national borders, and the smurfing of cash deposits followed by telegraphic transfers to other jurisdictions. In the non-bank financial sector, the use of bureaux de change or money remittance businesses to dispose of criminal proceeds remains the most often cited threat. Money launderers continue to receive the assistance of professional facilitators, who assist in a range of ways to mask the origin and ownership of tainted funds. The use of shell companies, usually incorporated in offshore jurisdictions, is the most common technique, with the use of accounts held by relatives or friends also being popular.

74. Several members had had difficulties in identifying the ordering customer in electronic funds transfer transactions. The focus of the problem varied from country to country. A recent study in one country showed that lack of customer identification information on the telegraphic transfer message was a significant problem, with up to 25% of messages from some jurisdictions not having the required ordering customer information. It was also noted that although sufficient information may be set out on the message, this did not mean it was accurate.

75. FATF members have continued to expand their money laundering laws to counter the new threats. The most common measures include extending the money laundering offence to non-drug related predicate offences, improving confiscation laws, and expanding the application of their laws in the financial sector to apply prevention measures to non-bank financial institutions and non-financial businesses. Increased efforts are also being made to make the administrative structures which deal with suspicious transaction reports more efficient and effective, and to improve international co-operation. However it was clear that further work needs to be done to improve international co-operation, particularly in relation to the speed with which information can be obtained at the investigative level.

76. The discussion held between law enforcement and regulatory experts from FATF members, e-money providers and issuers and a number of banking groups was an important step in a continuing process of co-operation to prevent new technology payments systems from being used by money launderers. Although FATF must continue to focus on identifying how criminals attempt to exploit existing financial payment systems, the clear results of the e-money discussion were that law enforcement and regulators must look forward to identify potential issues and new challenges now. Important features of these systems which may affect the degree to which they can be used by criminals include value limits placed on cards and Internet accounts, interoperability, transferability between individuals, disintermediation, and record keeping. Through cooperation and partnership with the industry, the FATF intends to continue to study this issue as payment systems develop, and to work to have effective and reasonable anti-money laundering measures implemented before the system is abused.

77. The global nature of the money laundering problem is clear, with all regions of the world being used by money launderers. In relation to regions where there are no FATF members, Eastern Europe, the former Soviet Union and Latin and South America were most often cited in money laundering cases, although money laundering is still a major threat in other areas of the world. A similar range of money laundering techniques and methods appears to be used in all regions, though the degree to which particular methods are used may vary depending on the size and sophistication of the financial markets and the counter measures that are in place. As in FATF countries, drug trafficking remains the major problem, though corruption, organised crime and fraud also generate huge proceeds. The development of counter-measures varies widely from region to region and country to country, though it is often closely linked to impact of international anti-money laundering initiatives in the area. What is evident though is that just as money launderers have moved their activities to less well regulated financial sectors, so is there increased movement to areas where the money laundering counter measures are weak. Whilst most FATF members and a few non-FATF countries have comprehensive measures in place, the vast majority of countries do not, and this is where increased attention needs to be focused.

February 1997

Annex 1

ANNEX TO THE FATF REPORT ON TYPOLOGIES - ISSUES CONCERNING NEW PAYMENT TECHNOLOGIES

I. INTRODUCTION

A. General

1. Following the adoption of new Recommendation 13 of the revised Forty Recommendations - "Countries should pay special attention to money laundering threats inherent in new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes" - this years typologies exercise started the process of addressing the issue. One of the purposes of the 1996-1997 FATF Typologies meeting held at the Organisation for Economic Co-operation and Development (OECD) in Paris on November 19 and 20, 1996, was to establish a dialogue among FATF members and leading international developers and providers of electronic banking and cash payment systems. Further, it was to provide representatives of the financial private sector an opportunity to answer questions regarding the operation of these systems and discuss issues of mutual concern with the international law enforcement and regulatory communities. The meeting followed on a FATF hosted meeting held in January 1996, called the Financial Services Forum, where representatives from governments and the private bank and non-bank sectors met to discuss anti-money laundering measures, including the issue of alternative payment systems.

2. The act of money laundering, while a crime in most countries, only occurs after an initial crime has been committed (such as fraud, drug trafficking, counterfeiting or any other specified unlawful activity which generates proceeds which need to be laundered). Further complicating the detection of this activity is the fact that the means by which the funds are laundered are not only legal, but commonplace activities such as opening bank accounts, purchasing monetary instruments, wiring funds, and exchanging currencies in international trade.

3. Electronic money (e-money) has the potential to make it easier for criminals to hide the source of their proceeds and move those proceeds without detection. And, it is safe to assume that if these new systems develop in such ways as to somehow better suit the criminals' needs than existing payment systems, they will use them.

B. Typologies Meeting

4. Therefore, while the Typologies Exercise concentrated specifically on money laundering, it was important to consider law enforcement concerns with respect to other crimes created by changes in payment systems technologies. For example, any type of financial institution, including an e-money system, could be extremely secure and resistant to compromise and in compliance with specified reporting/recordkeeping requirements, yet still could be used at any phase of the money laundering cycle.

5. Increasingly, FATF has been seeking to develop ways to increase co-operation with the private financial services sector. This approach becomes even more important with the advent of new e-money systems. Private sector experts invited by the FATF to the Typologies meeting presented an overview of the current technology developments in these payment systems and discussed the issues raised by law enforcement with respect to money laundering. The goals were to increase the knowledge of the FATF about the operations of these systems, advise the industry of law enforcement's potential concerns, and

ascertain what steps FATF and the industry could take together to ensure that these systems are developed in ways that minimize their potential abuse by criminals.

II. IDENTIFICATION OF ISSUES AND COVERAGE OF FATF RECOMMENDATIONS

6. The application of new technologies to electronic payment systems is still in its infancy. How these systems develop will depend on a combination of the effectiveness and efficiency of these technologies, the market and consumer acceptance. It should be noted that to date, there have been no reported instances of money laundering through these systems. Therefore, it is premature to consider prescriptive solutions to theoretical problems. However, it would be a disservice to the public and the developers of these new e-money systems for law enforcement and regulators not to continue to frame the issues that should be considered as markets and technologies mature. Therefore, described below are the FATF's efforts to identify the current types of e-money systems and discuss how they relate to existing payment systems, the 40 FATF Recommendations and general law enforcement and regulatory concerns.

A. Development of a Payment Services Taxonomy

7. In the broadest sense, payment systems are simply mechanisms to improve the usefulness of money, especially its ability to function as a medium of exchange. Thus, if e-money systems improve the effectiveness and have the potential to be more cost effective as providers contend that they will, this could represent a significant change in the way in which financial transactions will be conducted in the future. [1]

8. While to date, these new payment systems are focusing on low value consumer/retail transactions, it is prudent to recognise their potential broader impact. The technology exists which could permit these systems to combine the speed of the present bank-based wire transfer systems with the anonymity of currency. This combination has the potential to make wire transfer equivalents anonymous and permits currency to move around the world in seconds. E-money transactions also could be effected in multiple currencies without limits and conducted entirely without intermediaries.

9. Currently, there is no formally adopted international terminology with respect to e-money systems. Payment or transaction systems that use technologies such as stored value cards, "smart cards," and the Internet are often referred to by a variety of terms: "e-money," "digital cash," "cybermoney," "cybercurrency" and "cyberpayments." Often, the same term may have a different meaning depending upon context and circumstance. [2] Nevertheless, for purposes of discussion, three approaches to these new technologies were identified: stored value cards, network-based systems and hybrid systems.

(i) Stored Value Cards

10. Stored value cards use either magnetic, optical or chip technology. Although the value on magnetic and optical technology cards can be increased, they are not really considered viable vehicles for e-money due to limited security. The current state-of-the art in card technology is a card that uses a

[1] Cyberpayments: An Introductory Survey, the Financial Crimes Enforcement Network, U.S. Department of the Treasury, September 27, 1996.

[2] The October 1996 report prepared by the Bank For International Settlements (BIS) entitled: Implications for Central Banks of the Development of Electronic Money provides definitions and terminology. However, for purposes of the FATF Typologies Exercise , the terminology outlined in Section II of this paper was used.

microchip, as the chip provides greater security and is portable. Microchips are much more difficult to counterfeit or tamper with than optical or magnetic strips. This higher level of security makes such cards a much more acceptable "substitute" for physical currency. With these types of stored value cards the transfer of value takes place at the time and the place of the transaction; therefore, there is no operational need for immediate authorisation.

11. Some e-money systems use a variety of devices to facilitate transfers of value from one card to another, creating a decentralised network of payments. Some systems maintain records of each transaction (accounted), whereas it may be possible in some systems for individuals to authorise the transfer of "value" from one card to another "off-line" without authorisation (unaccounted).

(ii) Network-Based Systems

12. Some e-money systems use the Internet as the means of transfer. The global nature of the Internet removes the need for face-to-face meetings and allows anyone to perform a transaction with anyone else from anywhere in the world. Some systems require that there be an account held at a financial institution through which the value clears. Other systems contemplate the use of digital value or tokens, where the value is purchased from an issuer then stored on the computer rather than held in an account. The widespread availability of advanced cryptography makes it possible for these transactions to be completely secure. Even when a transaction leaves an "electronic trail" as it makes its way through the Internet, it may not necessarily be traceable back to a particular person or entity. These systems provide broad access, and their portability does not rely on physical transportation.

(iii) Hybrid Systems

13. All of these e-money systems employ sophisticated technologies to provide what are indeed very basic retail needs. The interrelationship of the different features and the rapid move toward system interoperability (where stored value cards and/or network-based systems are compatible with and accepted by each other) makes it difficult to identify distinct categories. Systems are now being developed that would allow stored value cards to be used interchangeably, regardless of issuer. Other developing systems would permit cards to be used in connection with network-based systems.

(iv) Main Characteristics of E-Money Systems

14. It is premature to make judgments about the extent to which any of the new payment systems discussed here will ultimately differ in kind from present-day systems. However, for purposes of discussion, there are some distinguishing characteristics among existing payment systems and e-money systems as well as among e-money systems themselves. Chart 1 in Appendix I lists "Some Simplified Generalizations" to help frame the current discussion.

15. Furthermore, the current distinctions between delivery of payment services via chip-cards and software-based Internet payment schemes are vanishing. E-money developers are designing chip-card interfaces for personal computers (PCs) that would facilitate the transfer of value from a chip-card to a PC. Since the development of these systems is dynamic and evolutionary, the most effective way to distinguish among systems is to focus on the issuing entity and whether the systems operate in an open or closed environment. The diagrams in Appendix II illustrate four e-money system models:

- Merchant Issuer Model - Card issuer and seller of goods and services are the same. Example: the Creative Star farecard used by riders of the Hong Kong Transit system.

- Bank Issuer Model for Closed and Open Systems - Merchant and card issuer are different parties. Transactions are cleared through traditional banking mechanisms. Example: Banksys' Proton card in Belgium and the Danmont card in Denmark.

- Non-Bank Issuer Model - In these systems users would buy electronic cash from issuers using traditional money and spend the electronic cash at participating merchants. The issuer will subequently redeem the electronic cash from the merchant. Example: CyberCash's electronic coin product.

- Peer-to-Peer Model - Bank or non-bank issued electronic cash would be transferable between users. The only point of contact between the traditional payments system and electronic cash would be the initial purchase of electronic cash from the issuer and redemption of electronic cash from individuals or merchants. Example: Mondex System.

16. This move toward interoperability makes it even more important that the way in which these systems are described and defined is done carefully. Definitions that are too broad might include services that are not really e-money and, therefore, of no particular interest or concern to law enforcement. Definitions that are too narrow, for example, by company as opposed to characteristics, will provide a different but equally important problem as certain systems may not be recognised until much later. Such scenarios could result in governments and providers taking action after the systems are implemented which is neither efficient nor cost effective. The FATF Typologies group agreed that it was important to continue a dialogue with the industry to ensure that there is an adequate understanding of the principal characteristics of these systems and their application to the FATF Recommendations and law enforcement and regulatory concerns.

B. Adequacy of Current Regulatory/Policy Initiatives

(i) Disintermediation/Changing Role for Necessary Intermediaries

17. Historically, law enforcement and regulatory officials have relied upon the intermediation of banks and other regulated financial institutions to provide "choke points" through which funds must generally pass and where records would be maintained. In fact, many anti-money laundering regulations as well as the FATF 40 Recommendations are designed specifically to require financial institutions to implement measures to ensure that a paper trail exists for law enforcement.

18. Recommendation 8 applies the FATF requirements to non-bank financial institutions. Recommendation 9 asks member countries to determine which other financial activities undertaken by non-financial businesses may be vulnerable to money laundering and, if so, to put in place effective controls.[3] E-money services probably could come under both of these recommendations.

19. Some e-money systems facilitate the exchange of financial value without the participation of a financial intermediary such as a bank. Thus, these systems tend to do away with the crucial "choke point" that aids law enforcement investigations. Therefore, as more becomes known about the operations of these systems, governments must identify what additional regulatory measures, if any, should be developed and implemented.

[3] Some examples listed in the Annex to Recommendation 9 of activities that could apply to e-money systems include accepting deposits and other repayable funds from the public, providing money transmission services, issuing or managing means of payment, and conducting foreign exchanges

(ii) The Role of Regulatory/Administrative Authorities

20. FATF Recommendations 26, 27, 28, and 29 describe the role of the regulatory or other administrative authorities with respect to evaluating and enforcing compliance with anti-money laundering measures. Another e-money issue is that some of these systems may be offered by entities who are not subject to existing established regulatory regimes. There is no consensus regarding the nature and extent of government oversight of e-money systems. Also, advancements in technology raise questions at to whether there is an effective or even feasible way to evaluate levels of compliance as are done currently with regulated financial institutions. The above-mentioned Recommendations assume such an ability.

(iii) Know Your Customer and Recordkeeping Policies/Identification of Suspicious Activity

21. Electronic money systems might make it difficult to "know your customer" with any degree of effectiveness or reliability. On the Internet, the largest international conglomerate and the smallest garage business may be indistinguishable, and, in both cases, next to nothing may be revealed about the organisation's actual activities. How will e-money providers effectively know their customers and how can suspicious activity be identified from the large number of anticipated transactions?

22. Several Recommendations would be difficult to apply to some e-money systems. For example, Recommendations 10-12 require financial institutions to keep certain transactional records as well as to verify and record the identity of individual customers and authenticate the legal structure of business customers. Also, reasonable measures should be taken to obtain and record information about the true identity of persons on whose behalf transactions are conducted or accounts opened. All such records should be maintained for at least five years and made available to the appropriate authorities when necessary. How measures like these could be implemented by e-money systems is a key issue. Further, Recommendations 14-19 require that financial institutions identify and report suspicious activity and develop and implement anti-money laundering compliance programs.

23. The transferability of e-money has a potential effect on money laundering. Some systems only allow for the transfer of value from an individual to retailers or to issuers, while others have the ability to allow for the transfer of value between individuals. Some system developers view these peer-to-peer transactions as a means to make e-money more of a cash equivalent. Others believe that such a feature increases the likelihood of fraud and counterfeiting. One way that e-money providers may address this problem is to permit only low value purchases to be transferred between individuals.

24. Value limits also have a potential effect on money laundering. Systems differ in the amount of value that may be held by an individual or a retailer on a chip or other device. While most tests of e-money systems have established limits ranging up to the equivalent of US$1,000, the technology exists to transact unlimited amounts.

25. Nevertheless, issuers probably would limit values stored on each device to reduce the risks of fraud. E-money systems could establish need-based limits which would be determined by commercial and market factors. For example, a retailer may have a larger value limit than an individual or even other retailers depending upon the volume of business. There also may be expiration dates that only permit value to be stored for a particular period of time before it would be necessary to re-clear the value with the issuer or deposit it back into an account. Or, electronic value could be programmed to expire after a certain number of transactions.

26. However, as with currency, monetary instruments and wire transfers, money launderers can be expected to exploit whatever limits are set, just as they do now by structuring transactions under currency reporting limits, obtaining multiple cards, using multiple names or employing multiple issuers.

27. The level of recordkeeping is an important law enforcement concern. Systems vary in the records kept both of individual transactions and of ownership. Some systems require very limited records while others maintain detailed records in a centralized database.

28. Transaction records: Transactions between individuals realistically cannot be centralized. And, even if technologically feasible, a record of each and every transaction would be cost prohibitive and provide huge masses of data of no commercial or law enforcement value. Detailed recordkeeping also has the potential to decrease customer acceptance because of privacy concerns. However, certain customers may want records of their transactions, and there may be records that e-money system operators keep for their own business purposes as well as to protect against fraud which could be employed also to combat money laundering.

29. Ownership records: Some systems would offer stored value cards through vending machines while others contemplate requiring that an account be opened and the owner identified in order to perform transactions. Obviously, the fewer records maintained, the more attractive the system might be to criminals.

(iv) Establishing A Balance Among Individual Privacy, Public Need For Security, And Legitimate Law Enforcement/Regulatory Access

30. The speed, security, and anonymity of e-money systems are positive characteristics that have the potential to protect the systems from compromise. However, these same characteristics may make these systems equally attractive to those who seek to use them for illicit purposes. Security and anonymity preserve privacy, which may be a vital component of effective and competitive business, yet have the potential to impede a law enforcement investigation from detecting illegal transactions. Further, Recommendation 2 states that financial institution secrecy laws should be conceived as to not inhibit anti-money laundering measures.

C. Effectiveness of Traditional Investigative Techniques and Analysis

31. E-money technologies will have an impact on the effectiveness of existing investigative techniques for financial crimes. These techniques were developed based on certain assumptions, such as the use of banks to make certain transactions, the ability of a financial institution to monitor its customers' activities and the use of physical currency. E-money systems challenge not only these assumptions about the nature of banking but also the way in which investigations are conducted.

(i) Less Vulnerability to Detection

32. The physical bulk of cash always has presented problems to the money launderer; it is not uncommon for money to be abandoned simply because it could not be moved quickly enough. E-money reduces the need for currency smuggling. Instead of a single shipping container or many false-bottomed suitcases, vast amounts of money could be transmitted instantaneously and securely with a few key strokes.

33. E-money systems create the potential to move money anywhere in the world without having to rely on a traditional depository institution as an intermediary. Funds could be moved to countries where

money laundering enforcement is weakest. Also, cards that have very high value limits would be easier to conceal than cash. Recommendation 22 specifically suggests that countries consider implementing measures to detect or monitor cross-border transportation of cash and/or bearer/negotiable instruments.

(ii) Rapidity of Financial Transactions Makes Monitoring More Difficult

34. The rapid movement of e-money (particularly over the Internet) will make it difficult for law enforcement to identify or track these fund transfers. Such payment systems combined with disintermediation also will make it difficult for regulators as well as law enforcement to establish programs to prevent money laundering.

(iii) Detection of Illegal Funds Hampered by Overall Volume of Activity

35. Currently, only a small portion of the daily $2 trillion worldwide volume of wire transfers is believed to be composed of illicit funds. Once e-money systems are used on a large scale, they also will handle a certain amount of these illicit funds. While it is not anticipated that e-money will consist of the same value as the wire system, it may consist of a larger volume of transactions, thus illegal funds may be even more difficult to find if only because of the sheer volume of funds circulating within the system.

36. The mass volume and the speed of processing of computerized data will make it difficult to develop indicators to detect suspicious activity. As an analogy, the Society for Worldwide Interbank Financial Telecommunications (SWIFT), a wholesale wire transfer clearinghouse, receives approximately 2.5 million messages per day, 580 million messages per year and has 135 member countries and 5,300 users. Also, SWIFT processes as many as a thousand transactions per second. [4]

37. Currently, on the Internet, there are an estimated 12.8 million host locations and 61.9 million users who generate more than a billion e-mail messages per month. These figures dwarf the SWIFT numbers and serve to illustrate how monitoring may be even more difficult in the e-money world.[5]

38. Recommendations 23 and 30 suggest that countries consider recording aggregate cash flows and the utility of implementing a currency reporting regime. With e-money systems, the above would be difficult and probably very expensive to implement.

D. International Jurisdictional Issues

39. For those e-money systems are being designed to operate internationally and in multiple currencies, another challenge facing law enforcement is the difficulty in determining jurisdictional authority. The current regulatory and law enforcement framework relies on defined financial and geographic borders. The diminishing of international financial borders makes it even more necessary to enhance cooperation and coordinate efforts among nations to ensure that there are consistent policies and standards. Recommendations 20, 21, and 32 refer to measures which would increase the application of international standards.

[4] Source: Fraud Working Group of the Banking Federation of the European Union's (BFUE) Explanatory Note: Electronic Payments Systems and Money Laundering, September 30, 1996.

[5] Hosts and e-mail information obtained from the Network Wizards Survey, July 1996, from the www.nw.com web site. User statistics from Anamorph's statistics generator, December 1996, obtained from the www.anamorph.com web site.

III. SUMMARY/FINDINGS

(i) Interoperability

40. There is no single design feature by itself that will make an e-money system attractive to criminals. E-money providers will consider a variety of factors in choosing their long term features with customer acceptance and concerns for fraud among the highest priorities. The evolution and ultimate design of these systems will be a determinant as to how attractive they are to money launderers. The combination of features chosen by e-money systems is affected by a number of factors including the business choices which reflect customer acceptance and prudent operation, the choices made by competitors and the existing legal and regulatory environment.

41. Clearly, efforts must be made to distinguish between issues that require resolution as the systems are being developed as opposed to issues which can be resolved on a case by case basis after the systems are in place.

(ii) The Role of Governments

42. In the analog world of finance, the private sector through innovation and adjustment has addressed many concerns that governments have raised without the need to create new regulatory requirements. At the same time, the public and the industry look to governments to set standards and provide a foundation and a level playing field upon which the private sector can operate. This is particularly important in light of the globalization of finance.

43. The same is true in the new digital world. The private sector is committed to working to resolve potential policy issues that may emerge. Accordingly, governments must react carefully to take advantage of market place solutions where suitable while maintaining expertise in this area to be in a position to act appropriately.[6]

(iii) Non-Bank/Non-Traditional E-Money Providers

44. Without disrupting the development of these systems, law enforcement and regulatory agencies must consider the new challenges posed by e-money providers other than banks. This challenge goes beyond the potential for disintermediation to include such issues as what government entity will have responsibility for ensuring adherence to anti-money laundering measures? What will the measures be? And, given the advanced state of technology, is there even a feasible way to effectively evaluate compliance?

(iv) Law Enforcement Techniques

45. Traditional law enforcement techniques and methods may become less effective or even obsolete. Law enforcement must begin to consider alternative approaches in addition to those in existence, to enhance their ability to prevent and detect money laundering as new payment system technologies gain world acceptance.

[6] An Introduction to Electronic Money Issues, prepared for the U.S. Department of the Treasury Conference: Toward Electronic Money & Banking, September 19-20, 1996, Washington, DC.

(v) Balancing Anonymity with Accountability

46. There must be an appropriate balance between an individual's right to financial privacy and the legitimate need of law enforcement and regulatory authorities to prevent and detect crime. The FATF has tried to achieve this balance as it has developed its Recommendations covering the existing financial services industry, but new technologies will create new challenges. Particular emphasis will need to be given to the practical ability of the providers to put measures in place without resulting in unnecessary costs and burdens.

47. The only effective way to do this is for the FATF to continue to work to bring law enforcement, regulatory agencies, and the private sector together to discuss issues of mutual concern. In this way, together we can develop effective and reasonable measures to prevent and detect financial crimes without impeding the commercial and consumer advantages of new technologies.

48. It was evident during the Typologies Exercise that the e-money industry wants and needs more feedback from governments in order to understand law enforcement concerns. This would enable them to incorporate possible solutions to perceived problems into their systems. It is also apparent that law enforcement must continue to reach out to the industry to increase its knowledge about the operations of these systems. FATF has a very valuable role and a major responsibility to continue to coordinate and facilitate communication between the e-money industry and the law enforcement/regulatory communities as well as among international organisations such as the Organisation for Economic Co-operation and Development (OECD), the Bank for International Settlements (BIS), the Basle Committee and others.

49. There are at present few, if any, statutes or regulations that specifically address e-money systems. Governments look to industry to keep abreast of the latest technological developments and in turn, must be willing to commit to provide adequate and timely feedback on responses and positions. Individual businesses or whole countries may compete to win customers by introducing e-money products and rules that have less stringent regulation. FATF should ensure a level playing field so that legitimate providers are not put at an economic competitive disadvantage.

IV. APPENDICES

Appendix 1 Chart 1: E-money Attributes: Some Simplified Generalizations for Discussion
Appendix 2 Diagrams 1-4: E-money Payment Models.

E-MONEY SYSTEMS ATTRIBUTES
SOME SIMPLIFIED GENERALIZATIONS FOR DISCUSSION*

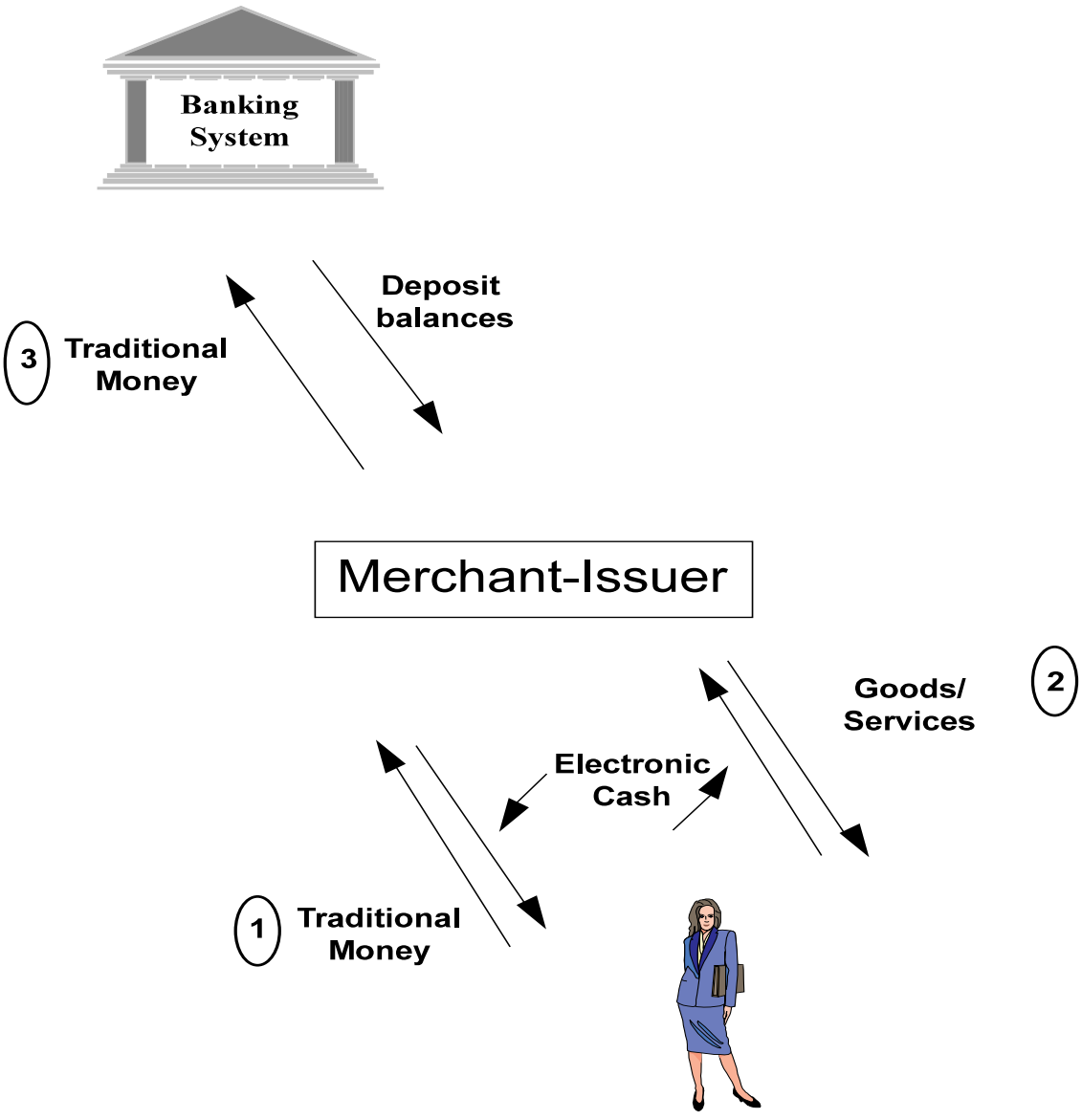
CURRENT PAYMENT SYSTEMS	E-MONEY SYSTEMS
High degree of central bank control	Various national views re: control
Highly structured supervision/regulation	Highly, technical yet to be designed
Large legal and policy literature	Applicability of existing laws/regs undetermined
Physical means of payment—checks, currency	Intangible electronic analogs
Huge infrastructure established worldwide	Downsized, computer-based
Relatively labor intensive	Relatively capital intensive
High value infrastructure—brick and mortar	Low cost decentralized facilities
Bank-dominated wire transfers	Personal computer transfers
Check-dominated consumer payments	Cybercurrency-dominated
Velocity of money is low	Velocity of money is high
Bank-dominated intermediaries	Non-traditional intermediaries
Clearing mechanism required	Clearing requirements reduced/eliminated
Transportation—couriers, land, sea, air	Telecommunications
Worldwide use of certain currencies	Easy currency exchange/one currency
Serial numbers and bank records	Enciphered messages
Significant statistical data collection	No methodology for money supply statistics
Economic national borders	Amorphous political & economic borders
Defined jurisdictions	Overlapping, unknown jurisdictions
Generally non-refutable, standard methods of validation	Evolving methods of transaction verification
Fungible	System specific convertibility to cash
Authentication, established structure to verify authenticity	Undetermined, system specific and may involve a third party

*These examples refer to the United States and are included for illustrative purposes only:

Source: Cyberpayments: An Introductory Survey, FinCEN, September 27, 1995

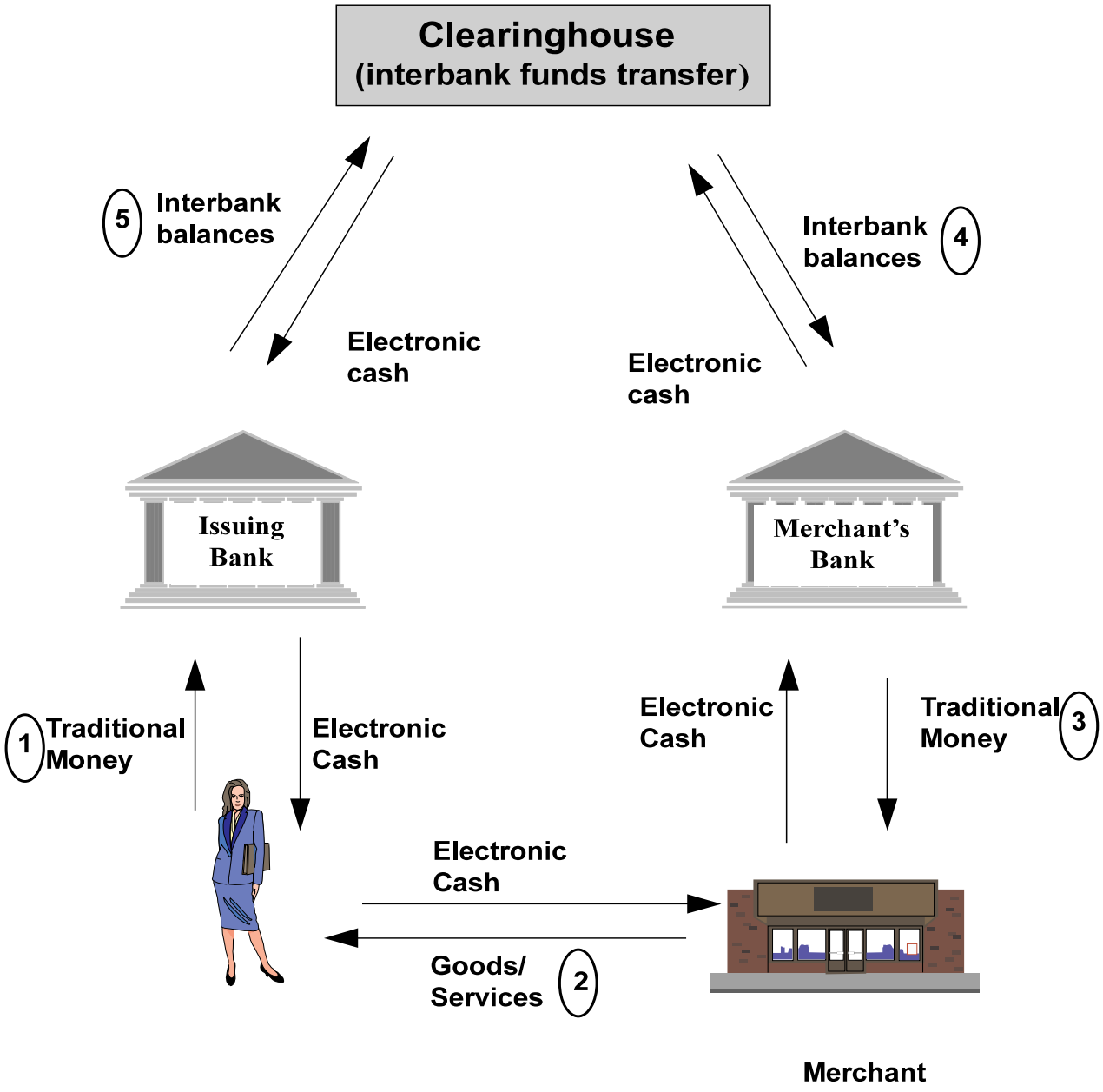
E-Money System:
Merchant-Issuer Model*

(Diagram 1)



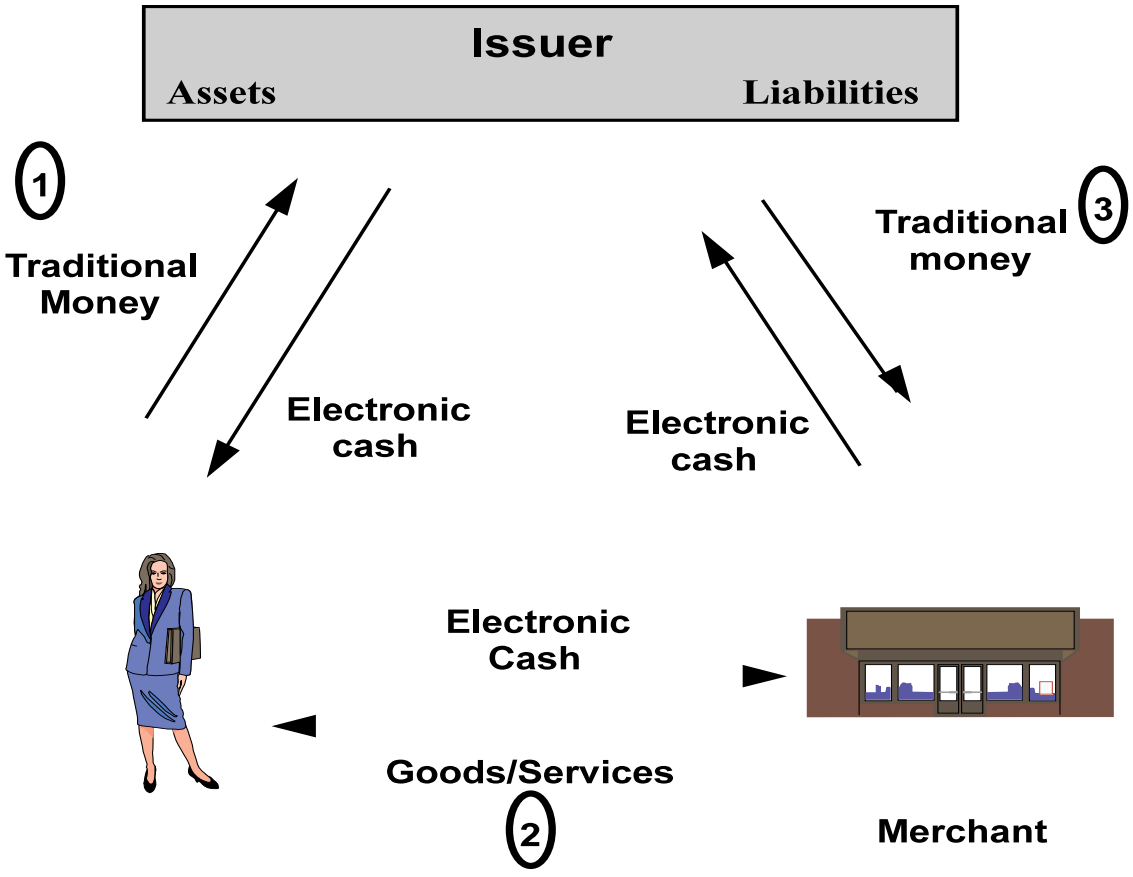
*This example refers to the United States and is included for illustrative purposes only.

E-Money System:
Bank Issuer Model for Closed and Open Systems*
(Diagram 2)



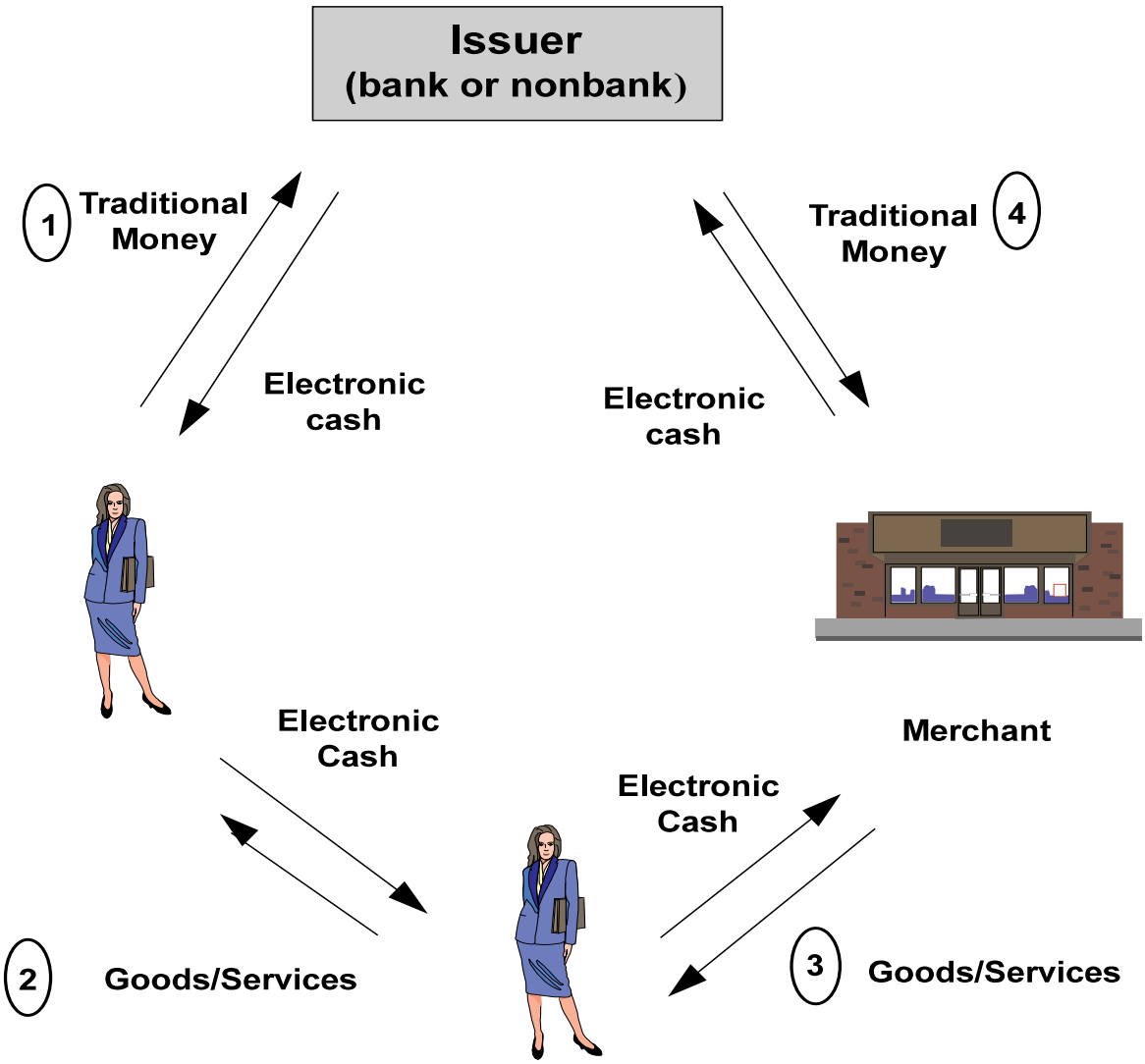
*This example refers to the United States and is included for illustrative purposes only.

E-Money System:
Nonbank Issuer Model*
(Diagram 3)



*This example refers to the United States and is included for illustrative purposes only.

E-Money System:
Peer-to-Peer Transfer*
(Diagram 4)



*This example refers to the United States and is included for illustrative purposes only.

ANNEX B

EVALUATION OF LAWS AND SYSTEMS IN FATF MEMBERS DEALING WITH ASSET CONFISCATION AND PROVISIONAL MEASURES

Introduction

1. This paper presents an analysis of members' responses to a questionnaire on measures taken by FATF members regarding the laws and systems they have in place as at 1 March 1997[1] in relation to confiscation and provisional measures, both under their domestic systems and pursuant to international mutual legal assistance. In addition responses were sought on the position of FATF members on three other topics - confiscated asset funds, co-ordination of seizure and confiscation proceedings, and asset sharing. Attached to this paper is Appendix 1, which sets out a table of the principal attributes or characteristics of members confiscation systems.

2. Confiscation is an important topic in relation to money laundering. The criminals' concern that their proceeds of crime may be confiscated is a major factor in motivating them to launder the proceeds of crime. An effective confiscation system is a necessary component of the anti-money laundering measures taken by any country. A considerable amount of qualitative information and a limited amount of quantitative information were provided in the answers to the questionnaire. This paper seeks to describe in general terms the nature of the systems which FATF members have adopted in regard to confiscation and associated provisional measures, both as regards domestic proceedings and in proceedings brought in response to a request for international mutual legal assistance. It will examine the results obtained from these confiscation systems, seek to identify areas of difficulty as well as fundamental strengths and weaknesses of various approaches. Finally there will be a similar description and analysis of any measures members have taken regarding confiscated asset funds, co-ordination of seizure and confiscation proceedings, and asset sharing.

I. DOMESTIC CONFISCATION SYSTEMS

3. All member countries have legislation providing for the confiscation or forfeiture of the proceeds or instrumentalities of some or all crimes, as well as provisions providing for the seizing or freezing of assets which may be subject to future confiscation. Money laundering is a criminal offence in all members, and it is also possible to confiscate the proceeds of that crime. There is a wide range and variety of confiscation laws and systems. Most members have enacted new confiscation legislation or made significant amendments in the last five years, such Switzerland in 1994, Greece in 1995, Ireland in 1994 and 1996, and Austria in 1997. Often, such members also still have older and more simply worded legislation which allows a court to confiscate the proceeds or instrumentalities of crime. Other countries such as Denmark have confiscation and ancillary provisions which are part of their general criminal code and have been in force without substantial amendment for many years.

Confiscation/forfeiture systems

4. A summary of the major features of members confiscation laws is set out at Appendix 1. For the purpose of this report the major characteristics of the confiscation or forfeiture provisions were whether :

[1] National laws and procedures are subject to change, and if information is sought on the laws of particular FATF members, then the national government of that country should be contacted.

a) the system was property or value based or both;
b) it applied only to drug trafficking offences or all serious crimes;
c) a conviction is required for the confiscation provisions to apply;
d) the standard of proof used in the proceedings was a criminal or civil (or some other easier) standard;
e) the burden of proof could be reversed so as to place an onus on the defendant to show that property was legitimately obtained or that he did not benefit from his criminal activity;
f) if a conviction is required, the confiscation or forfeiture order could be made in respect of the proceeds of crimes committed (but not prosecuted) before the offence of which the defendant is convicted or against assets acquired prior that time;
g) property owned by third parties (persons who are not defendants to the criminal proceedings) can be confiscated; and
h) property which is or is intended to be an instrumentality of the offence can be confiscated.

Property or Value

5. All members except Italy and Spain (which have only property based systems[2]) have systems which allow both for the confiscation of specific items of property which are found to be the proceeds or instrumentalities of a crime, and for the making of an order[3] based on the value of the proceeds of crime received. A large majority of the remaining members have systems where the principal method of confiscation is property based, but which allow for a value order to be made if that piece of property is not available for confiscation for certain reasons e.g. the defendant has removed it from the country and it cannot be located. With the exception of the Netherlands and Austria, the seven countries which have a value based system as their principal method of confiscation have a legal system based on English common law. Three members have systems which rely equally on property and value confiscation.

Drug trafficking offences or all serious crimes

6. Those members which have confiscation provisions which are part of the sentencing alternatives under their general criminal law normally have systems which cover all serious crimes, indeed all crimes. However, in addition, in certain countries the confiscation procedures are facilitated by laws such as reversing the burden of proof, which apply only to limited categories of more serious offences. Another group of members, such as the United Kingdom and the Netherlands has specific confiscation legislation which applies to all serious offences, whilst some others such as the United States and Canada have a list of more serious offences to which their confiscation legislation applies. Singapore has confiscation legislation which is limited to drug trafficking offences (including drug money laundering), and Luxembourg has specific confiscation legislation for drug trafficking and drug money laundering.

Necessity for conviction

7. All members have confiscation laws which are part of the sentencing proceedings of the defendant, and therefore a conviction is required. However, even though conviction based confiscation may be the normal type of confiscation used in a large majority of members, some members can also confiscate or forfeit property even though no conviction has been obtained. This can take place in two ways :

[2] Italy introduced value based confiscation for the offence of usury in 1995.

[3] Any reference to confiscation order is to be read as also referring to any decision or judgement of confiscation.

(a) confiscation within the context of criminal proceedings but without the need for a conviction or finding of guilt. For example, in England and Wales a confiscation order can be made if the defendant has absconded for at least two years, there is proof to the civil standard he has benefited from drug trafficking, and reasonable steps to contact him have been made. Similar, though not identical, provisions exist in most of the common law based countries. Other legislation in the United Kingdom provides a civil procedure within criminal proceedings whereby cash which is the proceeds or instrumentality of drug trafficking, and which is being imported or exported can be forfeited. In Austria, a confiscation order can be made in independent penal proceedings, where there is no formal finding on the guilt of the person;

(b) confiscation entirely outside criminal proceedings e.g. through civil or administrative proceedings. For example, in the United States, Germany or Ireland separate proceeding can be commenced provided the pre-conditions are met and a confiscation order made, even though there is no conviction. Provided there is a statutory basis to do so, a separate civil forfeiture proceeding may be brought in the United States provided there is probable cause to believe that property represents the proceeds or instrumentalities of crime. The civil forfeiture proceeding can occur independent of or parallel to related criminal proceedings. In addition, the United States has administrative, non-judicial forfeiture. In Ireland, civil proceedings can be brought to restrain and eventually confiscate property worth at least £10,000 which represents the proceeds or instrumentality of any offence. Italy also can bring non-criminal confiscation proceedings "in absentia" against the alleged offender on the authority of the court.

Standard of proof

8. Confiscation is normally regarded as part of the punishment of the defendant, although there are arguments which can be made that it also has a non-punitive purpose in some cases[4]. Being part of the penal proceedings it is therefore not surprising that the standard of proof applicable in most members is the criminal standard applicable to a sentencing hearing in their country[5]. In those eight members which follow an English common law system it is possible for the government to prove its case to the civil standard of the proof, which is easier to prove. In these countries it was felt that the criminal standard was too difficult to prove for serious crimes such as drug trafficking which have no victim who can readily identify the profits made by the criminal. Interestingly the Norwegian system requires that the prosecution must prove to the criminal standard that the defendant obtained proceeds from the offence, but is allowed to prove the value of those proceeds to the civil standard. In Denmark, if the amount of the proceeds cannot be sufficiently established then a sum thought to be equivalent to that amount may be confiscated. It should be noted that for some members which have a continental legal system their civil standard may be more difficult to prove.

4 Contrast the decision of the European Court in Welch v. United Kingdom, where the Court held that a particular confiscation under the Drug Trafficking Offences Act 1986 in England and Wales was punishment and a penalty, with the decision of the United States Supreme Court in United States v. Ursery which found that the civil forfeiture provisions in the United States are not punishment for double jeopardy purposes.

5 This can vary considerably e.g. in the United Kingdom and the United States the normal criminal standard for either conviction or sentence is "proof beyond reasonable doubt" (though the standard in a criminal drug forfeiture hearing in the United States is "the preponderance of the evidence"), whilst in France the normal criminal standard is the need for an "intime conviction".

Reversal of burden of proof

9. In the majority of members the burden of proving that assets are the proceeds of crime or that the defendant has derived a certain value amount as his proceeds of crime is placed on the prosecutor or the lawyer who represents the government. All but three of those ten members which allow the burden of proof to be placed on the defendant have legislated this power as a discretionary power which is held by the court, and which may usually be exercised when the government has presented some evidence to suggest that the asset may be criminally derived or that the defendant could not have acquired his assets taking into account his legitimate income. The United Kingdom requires the court to make wide-ranging assumptions about the illicit origin of property upon the request of the prosecutor in drug trafficking cases, and Hong Kong gives the court a discretion to do so. However, at present, there is no discretion to make these assumptions in drug money laundering cases. Australian legislation provides for automatic statutory forfeiture of the defendant's assets in drug trafficking or money laundering cases six months after conviction if the defendant does not prove they were legitimately acquired i.e. if the defendant does nothing the property is confiscated. Germany has a concept of extended forfeiture whereby for certain offences the State can seek to forfeit property of the defendant or an accessory, which is not directly linked to a specific offence, but which is subject to a justifiable assumption that it was acquired for or from illegal activity. In Austria the onus of proof may be partially reversed in cases where there has been repeated commissions of crimes over a period or where the defendant is a member of a criminal organisation.

10. France has two provisions which are potentially far reaching. The first relates to a person convicted of drug trafficking or drug money laundering, and it allows the court to confiscate all the defendant's property, whether legitimately acquired or not. The second provision was introduced in May 1996 and makes it a criminal offence for a person who carries on habitual relations with a drug trafficker or user to be unable to provide evidence of a legitimate source of funds commensurate with his lifestyle. If convicted then the person's property would be subject to confiscation. In this second case the burden of proof is thus reversed for the criminal offence itself, rather than in relation to the sentence. Italy also has provisions which ease the burden on the prosecutor. These provide that the property of a person who has been convicted of certain offences which relate to the Mafia, such as drug trafficking or extortion, can be liable to confiscation if the person cannot justify the origin of the property and it is disproportionate to the person's legitimate income. The confiscation proceedings can run parallel to the criminal proceedings or not, and the court can order that the amount which is disproportionate to legitimate income can be confiscated. Denmark has introduced a bill to require the defendant to render probable that his assets are legitimately acquired in cases of serious offences. Other members such as Belgium and Iceland are currently considering whether similar legislation should be introduced.

Link between conviction and confiscation

11. The issue is whether members can obtain an order for confiscation which only relates directly to the proceeds of crime from the criminal offence of which they have been convicted, or whether the confiscation order can also be sought in relation to the proceeds of previous crimes of which the person has not been convicted. Many countries, whether with a property or value system, which allow the burden of proof to be reversed can make a confiscation order which confiscates the proceeds of crimes other than for the offences of which the defendant is currently convicted. Some members which have a value based system of confiscation, whether as the primary or secondary system, indicated that they could enforce a monetary value order against any property, whether legitimately acquired or not. However this is an issue related to the enforcement of the confiscation order rather than the extent of the order itself. Canada and the Netherlands are unique in having a post conviction system which allows the confiscation of property which is the proceeds of previous crimes for which confiscation is allowed and which have not been prosecuted, but yet not having a provision which allows the burden of proof to be reversed. By contrast, France can confiscate such property for serious offences relating to drug trafficking, including drug money laundering, even if the property is legitimately acquired.

Third party property

12. A large majority of members have laws which, whilst respecting the rights of bona fide third parties, allow the confiscation of the proceeds of crime, or property of equivalent value in a value based system, from third parties who are not themselves defendants. Many members, for example France and Luxembourg, are able to seek confiscation of property held by persons who are accomplices or associates of the perpetrator of the predicate offence, for example, because they participated in, or hold the product of, that offence. However, such persons are not regarded as third parties for the purpose of this paper, since they are defendants in criminal proceedings. Examples of categories of situations where property held by third parties who are not charged with a criminal offence may be subject to confiscation are : where the person knew[6] that the property was derived from crime, where it was a direct or indirect gift from a defendant, or where the property was still subject to the effective control of the defendant. Turkey only confiscates property where it is owned by the criminal defendant.

Instrumentalities

13. The ability to confiscate the instrumentalities or products of a money laundering offence exists in almost all members, and is normally part of the general criminal law of the country. The only exceptions are Canada which cannot confiscate property used in the commission of a money laundering offence. Several members are unable to confiscate property which is intended to be used, rather than actually used, in the commission of such an offence (as required under Article 5(1) & (2) of the 1988 Vienna Convention).

Provisional measures

14. All members have legislation which provides their law enforcement agencies with the power to seize property which may become subject to a confiscation order as the proceeds of, or an instrumentality of a criminal offence. Similarly most jurisdictions have a power to freeze or obtain some form of order which secures such property, or in a value based system any property, so that a confiscation order could ultimately be enforced against the property. There does not appear to be any general difficulty with the operation of the legislation relating to provisional measures. All members are able to take provisional measures, either to seize or freeze, from the time that a person is arrested and charged with a relevant criminal offence until such time as the proceedings are concluded. Such powers can also be exercised prior to the person being arrested and charged in most members, though the seizure or freezing of the property can usually only be maintained for limited period of time if no charges are laid.

15. The power to order the seizure of the proceeds of crime is usually given to a prosecutor or investigating magistrate, and in some countries to a law enforcement official in exceptional circumstances. However, law enforcement officials are often empowered to seize property which is the direct proceeds or an instrumentality of the offence. The power to freeze, restrain or secure property is a judicial power which is normally reserved to the relevant court. To obtain such an order it is normally necessary to have sufficient evidence to satisfy the court that the person committed the offence and the person benefited from the offence or that the property is the proceeds of that offence. In a significant number of members it is also necessary to show that the freezing of the property is necessary in order to ensure that it will be available if a confiscation order is made i.e. a need to show a risk of dissipation.

6 Some countries may also have standards other than knowledge e.g. belief, suspicion, could not ignore etc.

Operational aspects

16. Approximately half the FATF members have dedicated financial investigation units within the police or another law enforcement agency which have a particular responsibility to investigate the financial aspects of crime (including money laundering), including asset identification and tracing with a view to confiscation. A proportion of these members also created further legislative powers to enable their law enforcement agencies to make the necessary financial investigations, usually because the existing powers to obtain information were limited to things which related to the offence itself and did not extend to what happened to the proceeds of the offence. Most law enforcement agencies engaged in investigating the financial position of the suspect conduct checks on the defendant's bank accounts, as well as checking public records relating to matters such as land ownership, companies, and motor vehicles. In many cases they are also able to obtain the person's tax records - this being important evidence to help in determining the person's legitimate income. The efficiency and speed with which the necessary financial inquiries can be done tends to depend on the degree to which public records are computerised - the ideal situation being that the investigating agency has on-line computer access to public records such as company or land records.

17. There are generally two possible purposes for these enquiries. One is to seek to prove that the property is the proceeds of the crime charged or some other illegal activity, or in a value system, that the defendant derived a certain benefit value from the offence. The other, which applies where the legislation allows the onus of proof to be reversed, is that investigator seeks to determine whether the defendant has assets the value of which are inconsistent with his known legitimate income.

18. There are a range of methods by which confiscation orders are enforced. In a majority of members the order operates to divest title to the asset from the previous owner and vest such ownership in the state. In other cases, such as with value orders, an agency of government has to take further steps to enforce the order against assets which can be used to satisfy the order. There are generally few difficulties as regards enforcement laws and procedures as the assets have normally been seized or frozen at an early stage of proceedings. The major problem area appears to arise when the assets are located outside the country, and mutual legal assistance is required to identify and freeze or seize the assets. However timely enforcement of confiscation orders can also be a problem.

Problems, proposed changes and aspects of the system that work well

19. One of the aspects of a confiscation system which was said to be very important is the issue of easing the burden of proof for the prosecutor. The issue here is the difficulty : (a) in proving to the criminal standard that the defendant has engaged in prior criminal conduct from which he has profited or obtained certain property, (b) linking the proceeds to specific prior criminal activity. This might not be difficult where the offence is one which has a readily identifiable victim, but most drug trafficking offences and many other serious offences have no direct victim who can give evidence, and moreover the many such offences involve the defendant being caught committing the crime, so that he has made no profit from that offence even though he may have been engaged in criminal activity for many years. The ability to reverse the burden of proof is regarded as a very important element of the systems in Australia, Hong Kong and the United Kingdom, whilst correspondingly Denmark, Germany, Iceland, Luxembourg, Norway and Sweden all consider the burden of proof to be a problem and some of them are considering reversing the burden for certain offences. Of interest are recent amendments to the law in Austria and Switzerland which allow the property of criminal organisations to be confiscated provided one can prove the organisation controls the property. It is not necessary to prove the illegal origins of the property.

20. A number of countries had a problem with the payment of legal expenses out of money which was frozen. The difficulty was reconciling the principle of the defendant's legitimate right to be legally represented using property which belonged to him with the practise whereby defendant's lawyers had in some cases used most or all of the frozen money on unmeritorious defences after which the defendant pled guilty. Some of the methods being considered to control the use of frozen money include : ensuring there is no other property available which could be used for this purpose, taxing the lawyers bills, preventing the use of assets which are actually the proceeds of crime, and requiring defendant's lawyers to be paid at legal aid rates.

21. Several countries also felt that they had benefited from an organisational structure where there was either a multi-disciplinary body or close co-operation between the relevant government departments or agencies. Canada, Finland, New Zealand, Norway and Singapore had all benefited from such arrangements, whilst one member indicated that there were some problems in the area of co-ordination which it would like to rectify. Similarly it was felt that an effective confiscation regime often requires prosecutors and investigators who are dedicated to this type of work.

22. In addition to the matters mentioned above, some members such as Luxembourg, Norway and Iceland were conducting a more general review of their confiscation laws. More than half the members consider that there are no problems with their system and are not proposing to make any changes.

Results obtained

23. Only 12 members kept statistics, and of these only nine had statistics on a year by year basis. Although a significant amount of money has been seized and confiscated in several countries, it is difficult to discern any clear trends on the statistics available. The statistics also have to be read with caution since countries may measure the number of confiscation/freezing orders in different ways, and one must also take into account the time lag between the commencement of a case (when the money is frozen) and its conclusion (when the money is confiscated). Many cases where property has been seized/ frozen are still continuing, and a confiscation order cannot be obtained until after conviction.

II MUTUAL LEGAL ASSISTANCE

24. FATF members are at differing stages of development as regards their systems of mutual legal assistance in relation to confiscation and provisional measures. Two members cannot provide assistance in this area, whilst other members are limited to drug trafficking or drug money laundering. Another two members cannot provide assistance on a full faith and credit basis, but have to commence their own domestic proceedings, whether a criminal prosecution for money laundering or civil in-rem confiscation for drugs and a range of other serious offences linked to terrorism or fraud.

25. Traditionally, mutual legal assistance in relation to confiscation can be divided into three broad areas: (a) investigative assistance to identify and trace property and obtain documents, (b) the ability to freeze or seize property pursuant to a request based on a confiscation order which will be obtained in the foreign jurisdiction, and (c) the ability to register and enforce that foreign confiscation order. Most members have had a number of requests for investigative assistance, whether requiring the use of coercive measures or not. Usually a formal request is required if coercive action is to be taken, however some members such as the United Kingdom can obtain search warrants or production orders for documents on a law enforcement agency to agency basis. Most members however, have had very little experience in relation to freezing, seizing and confiscation assistance. In some cases information is not

available because statistics are not kept - only 6 members have information on the number and value of mutual legal assistance requests made and received. However, many members have simply not made or received requests for mutual assistance to freeze or confiscate property. Given this limited experience, few problems have been identified and not many members are currently considering changes.

Conduits for assistance

26. Leaving to one side traditional methods of assistance such as letters of request, most of which relate to the obtaining and taking of evidence for criminal proceedings, and informal assistance between law enforcement agencies whether on a bilateral basis or through organisations such as Interpol or World Customs Organisation, there are three principal methods by which members are able to give assistance :

(a) multilateral conventions -

- the 1988 Vienna Convention (the 1988 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances)[19 members have ratified and three intend to do so within the near future];
- the 1990 Convention of the Council of Europe on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime [ten members have ratified and six more intend to do so within the near future];
- the 1970 European Convention on the International Validity of Criminal Judgements;
- the 1959 European Convention on Mutual Assistance in Criminal Matters;

(b) bilateral agreements - usually to ensure that the bilateral partner can offer reciprocal assistance;
(c) pursuant to their own domestic laws whether on the basis of reciprocity, dual criminality or otherwise.

Types of assistance

27. **Investigative** - all members are able to provide assistance in money laundering cases in taking coercive measures to search for and seize documents and records, whether held by financial institutions, companies or individuals. This covers identifying and tracing the proceeds of crime with the ultimate object of confiscation. Apart from Italy these members can also obtain an order which requires documents to be produced, although such documents can be obtained in Italy by seizure. One unusual investigative tool, which is probably of more value to a criminal prosecution for money laundering than for the confiscation aspect of the case is a monitoring order. In Australia, Hong Kong and New Zealand the authorities can apply for an order in relation to drug trafficking and money laundering offences which allows them to obtain not just historical information (a production order) but also current and future (yet to be created) banking documents and information. Such an order is a form of financial surveillance which can compel a financial institution to provide information and documents about a particular person or account as and when those documents are created for a future period of up to three months, and could be a useful tool in determining when criminality is about to take place.

28. There is no common set of conditions under which assistance can be provided, and members did not indicate that there are particular difficulties which prevented or inhibited assistance in this area. However two issues which appear to be a problem for some countries are : (a) many members require a multilateral or bilateral basis to provide assistance, and insufficient countries are able to take

action pursuant to these channels, and (b) insufficient information is provided to the requested country to satisfy its criteria i.e. the request appears to be "fishing" for information. An aspect that appears to be working well in the United Kingdom and Hong Kong is the capacity in drug cases for law enforcement agencies to obtain production orders and search warrants on behalf of foreign law enforcement agencies and provide them with copies of documents without the need for a formal request under a convention or agreement, dual criminality, reciprocity or many of the other usual preconditions. At an investigative level this allows documents to be obtained expeditiously allowing complicated international money laundering inquiries to proceed much more quickly.

29. **Freezing/Seizing** - a request for assistance in relation to one of these two types of provisional measures, or for an order for security to be obtained over the property in question can be acted upon in 22 members. The United States and Canada may also be able to assist using their own domestic confiscation proceedings. New Zealand is able to register and enforce a foreign freezing order, but other members act upon the request, and if the necessary conditions are fulfilled they can take action to freeze or seize on the basis of their own legislation, which does not require any provisional measure to have been taken in the foreign jurisdiction. Examples of conditions commonly necessary to give effect to such requests are :

- the need for a multilateral or bilateral conduit under which the request can be made;
- dual criminality - the conduct must amount to a criminal offence in both countries;
- that the relief sought could also be obtained if those proceedings had been brought in the requested country;
- there is sufficient evidence to show that a confiscation order could ultimately be made in the requesting country.

However some members such as Denmark, France or Portugal can provide assistance for provisional measures even though there is no bilateral or multilateral agreement, provided the necessary criteria are met.

30. An interesting feature of co-operation between Luxembourg and the United States has been the freezing of assets held in Luxembourg, with the subsequent repatriation of those assets to the United States where they have been forfeited. Also of note is the ability of several FATF countries to order repatriation to the requesting country of any assets held in the requested country that are an object of the offence (including those held in bank accounts) and which are controlled by the person who is being extradited.

31. **Confiscation** - A number of members have limitations to their ability to assist in enforcing a foreign confiscation order. Seven members cannot register and enforce a foreign confiscation order. Spain is unable to register a foreign value confiscation order, though it can register a property based order relating to the direct or indirect proceeds or instrumentalities of the crime as well as any income earned from the offence. Hong Kong, Luxembourg, Japan and Singapore are currently limited to drug offences. Once the foreign confiscation order is registered it is enforced in the same way as a domestic order, whether by enforcing a property confiscation order directly (since the title to the property passes to the State with the confiscation order) or by appointing receivers or using some other method of civil or criminal enforcement for value based orders. In 15 members the confiscated monies are paid into General Revenue, whilst in seven members the money is either paid into an asset forfeiture fund or may be available to share with the requesting country in certain circumstances. In addition to the conditions mentioned in paragraph 29 above, other common pre-requisites in order to register a foreign confiscation order are :

(a) the order must be final and not subject to any appeal;
(b) the defendant must have had an opportunity to appear at the proceedings in the requesting country and be legally represented there;
(c) it must not be contrary to any other fundamental principles of justice in the requested country.

Problems, proposed changes and aspects of the system that work well

32. Members were unable to identify many specific problems that they had with their systems of mutual legal assistance. However, given the limitations of one type or another which apply to most of the members systems, the lack of problems may be due more to lack of experience (and thus not having cases from which problems arise) than necessarily having a perfect system. Some of the fundamental problems for members appear to be :

(a) not having ratified the multilateral conventions or agreed to bilateral agreements under which they could make requests for assistance and not having the necessary domestic legislation in place. The 1988 Vienna Convention, which is limited to drug offences, has been ratified by 19 members but it is important that all members ratify it promptly. The 1990 Council of Europe Convention, has been ratified by only a limited number of FATF members. Given the comprehensive and recent nature of this Convention it is very desirable that members which are able to do so, should take early steps to sign and ratify it. A limited number of members use bilateral agreements to any great extent, and even those which do, such as Australia and the United Kingdom, have had very few confiscation cases. Similarly France, which relies on multilateral and bilateral agreements for confiscation had few cases requesting confiscation related mutual legal assistance in 1995. However, the extension of the money laundering offence in France to cover all crimes means it is now able to provide assistance on a much wider basis.

(b) the limitations of domestic legislation are recognised as being problems. Canada and the United States have noted that the need for them to commence their own domestic prosecution or confiscation case is a problem. The United States is therefore proposing measures to allow foreign governments to enforce their own value confiscation orders in United States courts. It also proposes creating a power to freeze property for thirty days if it is owned by a defendant charged in a foreign country, when the property could be forfeited under United States law. Correspondingly, the United States is concerned that some FATF members may not be able to enforce a civil forfeiture order made in the United States, since there is no conviction. This may be the case in members which require all the pre-requisites for domestic confiscation (including conviction) to be met. A number of members are taking or considering further steps - Belgium has introduced legislation to allow mutual legal assistance in relation to confiscation and related matters, Hong Kong is preparing legislation for full mutual legal assistance for all serious crimes, France is now able to provide assistance in relation to confiscation for non-drug money laundering, whilst Norway and Iceland will both be reviewing their current legislation.

33. Some of the other problems identified were - some countries were concerned about the speed at which requests for assistance were actioned, thus giving the criminals the opportunity to transfer the property to another country and avoid it being frozen or seized. Australia recognised that it could not freeze property prior to charge and is thus making the necessary amendments, whilst Canada felt that pre-charge restraint orders created problems for countries which required any request to issue from a judicial authority. Generally however, despite the lack of cases and statistics and the problems identified above, most members did not feel that their systems had any problems and were not proposing to make any changes.

Results

34. What is noticeable is that most members have had no or very few requests for assistance even when they have the necessary legislation in place. The available statistics do not allow any particular conclusions to be drawn. In those members which have received or made requests the reduction from the amount frozen/seized to the amount confiscated or realised may be due to the fact that cases are ongoing, and that the confiscation stage has not been reached.

III CONFISCATED ASSET FUNDS, CO-ORDINATED ACTION AND ASSET SHARING

Confiscated Asset Funds

35. Only seven members - Australia, Canada, Italy (for the proceeds of drug trafficking only), Luxembourg, Spain, the United Kingdom and the United States have confiscated asset funds. These are specific funds held by the government into which the amounts realised from the sale of confiscated assets are paid. The monies held by the fund can then be used for purposes such as sharing with other countries or provincial governments within the country, law enforcement projects, and drug rehabilitation and education. The United Kingdom only deposits monies received from international cases into its fund i.e. those obtained when a foreign confiscation order is registered and enforced or gifts from overseas countries in connection with joint investigations where confiscation has resulted. This amounted to some £ 4.7 million over the last six years. The other four countries put all their confiscated assets in the fund. All these members thought that their funds were working well and were very helpful in promoting international and inter-agency co-operation. The remaining members did not have such a fund, and except for Belgium and the Netherlands are not considering one. The main reason for not having a fund in almost every member is that it is contrary to the normal budgetary principles of government and leads to a hypothecation of revenue. The normal principle of course being that all monies raised by government are put into general revenue and all disbursements are then made from there.

Co-ordination of seizure and confiscation proceedings

36. The issue is whether a member can liaise and co-ordinate with another jurisdiction usually prior to, but occasionally after proceedings commence, so as to take the most effective action to freeze and seize as well as confiscate the proceeds of crime. In most cases this will simply be an extension of members ability to conduct co-operative investigations, which is something that all members can do, and will involve making a decision as to where a person will be prosecuted or the confiscation proceedings brought. At least 20 members have the ability to co-ordinate their proceedings, as well as having policies and procedures in place. At least half of these either required this co-ordination to take place pursuant to mutual legal assistance arrangements, or felt that it was desirable that it should do so. However only two members have specifically had cases where they have had to co-ordinate their seizure and confiscation proceedings with another jurisdiction, and thus members did not have any specific problems which they were aware of.

Asset Sharing

37. Sixteen members can share confiscated assets, whilst seventeen are able to receive such assets. In a large majority of these countries there is no specific law which allows this, but on the other hand there is nothing to prohibit it. Most countries do however require such sharing or receipt of confiscated assets to be made pursuant to a mutual legal assistance agreement. Some of the other preconditions which are necessary before sharing can take place are :

(a) a restriction which applies to Australia and presumably most other members is that sharing and receipt of assets applies only to cases where the assistance is pursuant to a request to freeze/seize or confiscate assets. It does not extend to situations where the only assistance provided is investigative assistance. However, the United States and the Netherlands do share for cases of both judicial and investigative assistance;
(b) as a matter of policy one member will only consider sharing in cases where the assets are worth more than US$ 1.3m;
(c) another member can only share if property is confiscated and not in relation to cash (value) confiscation.

Outside the United States there has been little actual experience of asset sharing, though Luxembourg, the United Kingdom and Switzerland have both received and shared assets.

IV CONCLUSION

38. It has been said that certain criminals and criminal organisations do not mind convictions or prison sentences provided they are able to retain their ill-gotten gains. An effective confiscation system, both domestically and internationally, is therefore a very important deterrent to criminal activity, as well as being cost effective. As can be seen from Appendix 1 there are a diversity of confiscation systems, with many different features. This fact, combined with a lack of statistics, and a lack of experience in many countries, makes it difficult to isolate problems let alone identify desirable attributes of an ideal system. Two points which are important to consider though are that :

(a) many forms of profit making crime, and particularly drug trafficking, are engaged in by criminals as a long term business activity. Only confiscating the proceeds of the crime for which they are actually caught is unlikely to deprive them of a substantial proportion of their illegal profits;

(b) for most serious offences such as drug trafficking, organised crime or complex fraud it will be difficult, if not impossible, to prove to the normal criminal standard the extent to which a defendant has benefited financially from his criminality.

39. Most countries have had confiscation laws for many years, but these are limited systems of "classic" seizure and confiscation laws. They are able to deal with simple cases where, for example, the drug trafficker is caught with the drugs and the proceeds of his most recent sale, but it is questionable whether older, simpler laws of this nature are sufficient. There are a number of additional measures which governments should consider if they want to effectively confiscate, seize and freeze laundered proceeds and deal with the considerations mentioned in paragraph 38 above. Some measures should be implemented in all members : (a) an effective confiscation scheme should extend to a range of serious offences and not just drug trafficking, especially to prevent the defence argument that the property is the proceeds of another form of crime than drugs; (b) it should also be possible to take action in appropriate cases to confiscate the proceeds of crime (or property of an equivalent value) even if it is in the name of third parties, and countries which require such laws could consider some of the alternative methods for dealing with this issue set out at paragraph 12 above. Although the United States has a powerful and effective tool in its civil forfeiture proceedings, most countries require a conviction before they can take action to confiscate property. Members should give consideration to non-conviction based confiscation or the more limited alternative that where confiscation is conviction based, members consider laws which allow them to take freezing and, where possible, confiscation action against absconders or fugitives from justice. A defendant who is a fugitive should not also have the benefit of retaining the proceeds of criminal conduct.

(a) a restriction which applies to Australia and presumably most other members is that sharing and receipt of assets applies only to cases where the assistance is pursuant to a request to freeze/seize or confiscate assets. It does not extend to situations where the only assistance provided is investigative assistance. However, the United States and the Netherlands do share for cases of both judicial and investigative assistance;
(b) as a matter of policy one member will only consider sharing in cases where the assets are worth more than US$ 1.3m;
(c) another member can only share if property is confiscated and not in relation to cash (value) confiscation.

Outside the United States there has been little actual experience of asset sharing, though Luxembourg, the United Kingdom and Switzerland have both received and shared assets.

IV CONCLUSION

38. It has been said that certain criminals and criminal organisations do not mind convictions or prison sentences provided they are able to retain their ill-gotten gains. An effective confiscation system, both domestically and internationally, is therefore a very important deterrent to criminal activity, as well as being cost effective. As can be seen from Appendix 1 there are a diversity of confiscation systems, with many different features. This fact, combined with a lack of statistics, and a lack of experience in many countries, makes it difficult to isolate problems let alone identify desirable attributes of an ideal system. Two points which are important to consider though are that :

(a) many forms of profit making crime, and particularly drug trafficking, are engaged in by criminals as a long term business activity. Only confiscating the proceeds of the crime for which they are actually caught is unlikely to deprive them of a substantial proportion of their illegal profits;

(b) for most serious offences such as drug trafficking, organised crime or complex fraud it will be difficult, if not impossible, to prove to the normal criminal standard the extent to which a defendant has benefited financially from his criminality.

39. Most countries have had confiscation laws for many years, but these are limited systems of "classic" seizure and confiscation laws. They are able to deal with simple cases where, for example, the drug trafficker is caught with the drugs and the proceeds of his most recent sale, but it is questionable whether older, simpler laws of this nature are sufficient. There are a number of additional measures which governments should consider if they want to effectively confiscate, seize and freeze laundered proceeds and deal with the considerations mentioned in paragraph 38 above. Some measures should be implemented in all members : (a) an effective confiscation scheme should extend to a range of serious offences and not just drug trafficking, especially to prevent the defence argument that the property is the proceeds of another form of crime than drugs; (b) it should also be possible to take action in appropriate cases to confiscate the proceeds of crime (or property of an equivalent value) even if it is in the name of third parties, and countries which require such laws could consider some of the alternative methods for dealing with this issue set out at paragraph 12 above. Although the United States has a powerful and effective tool in its civil forfeiture proceedings, most countries require a conviction before they can take action to confiscate property. Members should give consideration to non-conviction based confiscation or the more limited alternative that where confiscation is conviction based, members consider laws which allow them to take freezing and, where possible, confiscation action against absconders or fugitives from justice. A defendant who is a fugitive should not also have the benefit of retaining the proceeds of criminal conduct.

40. Probably the single most important issue though for most members is the question of the burden of proof upon the government and whether it can be eased or reversed. Integrally linked is the question of depriving a defendant of proceeds of offences other than those for which he is immediately convicted. If the aim of governments is to strip a convicted defendant of all his criminal proceeds, then they should seriously consider measures to make the task easier for the prosecutor. Measures that should be considered include:

- applying an easier standard of proof than the normal criminal standard to the confiscation proceedings;
- the more effective alternative of reversing the burden of proof and requiring the defendant to prove that his assets are legitimately acquired;
- if a conviction is required for confiscation, enabling the court to confiscate the proceeds of criminal activity other than the crimes of which the defendant is immediately convicted.

Subject to the fundamental principles of each country's domestic law, and to a need to preserve the rights of victims, members should consider enacting such measures in relation to serious criminal activities such as drug trafficking or organised crime. Another option, as enacted in France, is to give the court a discretionary paper to confiscate the assets of a person convicted of serious offences relating to drug trafficking, or as in Italy, to require the court to order the confiscation of all assets which are disproportionate to the person's legitimate income.

41. There is generally no particular difficulty with provisional measures, though the issue of release of funds for the defendant's legal expenses does raise difficult questions of public policy, and it is questionable whether prosecutors should be required to prove a risk of dissipation. In order to ensure that any confiscation order which is ultimately made can be enforced against available assets members should be able to freeze/seize all types of property from the earliest stage of the criminal proceedings until they are concluded. As regards operational issues an effective confiscation regime will usually require prosecutors and investigators who are dedicated to this type of work. Lack of dedicated resources will always mean that there will be more urgent priorities elsewhere since asset confiscation is often regarded as ancillary to mainstream prosecutions.

42. As regards mutual legal assistance the primary difficulties seem to be that insufficient members have ratified the Vienna or Strasbourg Conventions, or they do not have the necessary domestic legislation in place. International drug trafficking clearly generates a large amount of money as can be seen from the amount confiscated in some countries, however there has been very limited mutual assistance experience amongst members in the confiscation field. Since international co-operation is the focus of a lot of work amongst law enforcement agencies, the capacity to take the necessary legal and judicial steps must keep pace. Asset sharing and co-ordinating seizure and confiscation proceedings are also aspects of international co-operation which are in their infancy at present. A majority of members can share assets and co-ordinate proceedings, but very few have any practical experience. International co-operation generally should be subject to further detailed study in the future.

43. In conclusion, steps need to be taken both to ensure that an effective domestic confiscation regime is put in place which strips criminals of the proceeds of all their criminality, wherever they may have put it, and that increased efforts are made to improve the level of mutual legal assistance.

CHARACTERISTICS OF NATIONAL LEGAL SYSTEMS FOR CONFISCATION

Explanation

Year: - The year of enactment of the confiscation legislation or the last major amendment
Drugs or Serious Crime: - Does the legislation apply only to drugs or to all serious crime
Property or value: - Does the confiscation law principally confiscate items of property (Property) or does it provide that the person pay a sum of money (Value) [principal and most used method is in bold type]
Conviction required: - Is a conviction required before confiscation can be sought, or is it possible to confiscate without a conviction (either in a wide or limited range of cases)
Reverse burden of proof: - Is it mandatory or discretionary for the court to reverse the burden of proof so that the defendant or owner of the property to be confiscated must prove that the property (or the alleged benefit from the crime in a value system) is not acquired from crime
Proceeds must be linked to conviction: - Does the confiscation law allow a person to be deprived only of the proceeds of crimes for which he is convicted?
Third party property: - Many countries prosecute an accomplice or associate of the defendant who commits the predicate offence, but criminal defendants are not included as "third parties" in this annex. This column sets out three categories of situation (this is not an exhaustive list) where property which is owned or held by third parties can be confiscated or made subject to the confiscation order.
(i) gift - property is given to the 3rd party by the defendant for little or no real consideration;
(ii) knowledge - if the 3rd party knew, believed, suspected, could not ignore etc., that the property was the proceeds of crime;
(iii) effective control - the defendant still effectively controlled the property at the time of the confiscation proceedings, whoever the nominee owner is.

Country	Year	Drugs (D) or serious crime (SC)	Property or value confisca-tion	Convic-tion required?	Criminal or civil (or other easier) standard of proof	Reverse burden of proof ?	Proceeds must be linked to conviction	Third party property
Australia								
- Customs Act	1979	D	**PV**	no	civil	no	no	eff. control
- POCA	1987	SC	**PV**	yes [1]	civil	yes	no	eff. control
Austria	1997	SC	**PV**	no	criminal	yes[2]	no	gift
Belgium	1990	SC	**PV**	yes	criminal	no [3]	yes	yes
Canada	1989	SC	**PV**	yes	both possible	no	no	yes
Denmark	1930s	SC	**PV**	yes [4]	criminal	no[5]	yes	all categories
Finland	1994	SC	**PV**	yes	criminal	no	yes	yes
France		SC	**PV**	yes	criminal	yes (drugs)[5]	no (drugs) [6]	knowledge
Germany	1975	SC	**PV**	no	criminal	no [7]	yes [6]	yes
Greece	1995	SC	**PV**	no	criminal	yes	no	gift
Hong Kong	1995	SC	**PV**	yes [8]	civil	yes	no [8]	gift/eff. control
Iceland	1940s	SC	**PV**	no	criminal	no [4]	yes	knowledge
Ireland	1994	SC	**PV**	yes	civil	yes	no	gift
	1996	SC	**P**	no	civil	yes	no	yes

Country	Year	Drugs (D) or serious crime (SC)	Property or value confisca-tion	Convic-tion required?	Criminal or civil (or other easier) standard of proof	Reverse burden of proof ?	Proceeds must be linked to conviction	Third party property
Italy	1950	SC	P	yes[9]	criminal	yes[10]	no[9]	eff. control
Japan								
- Penal Code	1908	SC	**P**V	yes	criminal	no	yes	knowledge
- Anti drug law	1992	D	**P**V	yes	criminal	yes[11]	yes	knowledge
Luxembourg	1989	SC	**P**V	no	criminal	no	yes	yes
Netherlands	1993	SC	P**V**	yes	other [12]	no	no	yes
Neths. Antilles		SC	P**V**	yes	criminal	no	yes	yes
Aruba		SC	P**V**	yes	criminal	no	no	yes
New Zealand	1992	SC	**PV**	yes [1]	civil	yes [10]	yes	eff. control
Norway	1985	SC	**PV**	no	criminal/civil	no	yes	gift/knowledge
Portugal	1995	SC	**P**V	yes	criminal	no	yes	knowledge
Singapore	1993	D	P**V**	yes	civil	yes	no	gift/eff. control
Spain	1996	SC	P	yes	criminal	no	yes	yes[13]
Sweden	1940s	SC	**P**V	yes	criminal	no	yes	yes
Switzerland	1994	SC	**PV**	no	criminal	yes	no	yes
Turkey	1920s	SC	**P**V	yes	criminal	no	yes	no
United Kingdom	1995	SC	P**V**	yes [8]	civil	yes	no [8]	gift
United States								
- civil forfeiture	1986	SC	P	no	civil	yes[15]	no	know/eff. cont'l
- crim. forfeiture	1984	SC	**P**V	yes	criminal[14]	no	yes	gift/eff. control
TOTALS		**D: 1** **SC: 25**	**P: 16** **V: 6** **PV:4**	**Yes: 17** **No: 7** **Both: 2**	**Criminal: 16** **Civil: 6** **Both: 3**	**Yes: 11** **No: 13** **Both: 2**	**Yes: 13** **No: 12** **Both: 1**	**Yes: 25** **No: 1**

[1] Australia and New Zealand - except for persons who die or abscond prior to conviction, who may be deemed convicted for confiscation purposes.

[2] Austria - the onus of proof may be partially reversed in cases where there has been repeated commissions of crimes over a period or where the defendant is a member of a criminal organisation.

[3] Belgium - considering whether to reverse burden as part of measures to be taken against organised crime.

[4] Denmark - an order can be made w/o conviction if there is no prosecution because the limitation period for the offence has expired.

[5] Denmark has introduced a bill and Iceland is considering whether to introduce a bill which requires the defendant to render probable that his property was legitimately acquired for serious offences.

6 France - the court can order that a defendants property is confiscated (whether acquired before or after the crime and whether legitimate or not) if the defendant is convicted of a drug trafficking or drug money laundering offence. The property is confiscated without need for the prosecution to do more than obtain a conviction.

7 Germany - if the defendant is convicted of certain offences the court may assume that assets of the defendant were acquired from illegal activity if the circumstances justify this, and may thus confiscate them.

8 Hong Kong and United Kingdom - a confiscation order can be made without a conviction where the defendant absconds or dies prior to conviction. In addition, cash which is imported or exported and is the proceeds or instrumentality of drug trafficking can be forfeited without a conviction.

9 Italy - in certain cases one can have confiscation without conviction.

10 Italy - for drug trafficking and organised crime the onus of proving the assets are legitimate can be placed on the defendant if his assets are not commensurate with his income. In such cases it can apply to any assets, and not just to those which are the proceeds of the offence of which he is convicted.

11 Japan and New Zealand - for drug offences if the property was obtained during the period of the offences and the value of the property is not commensurate with the defendant's legitimate income.

12 Netherlands - the standard of proof is slightly easier than the full criminal standard.

13 Spain - property can be confiscated where it is a gift and the third party knew or suspected that it was the proceeds of crime. Similarly, a confiscation order can be executed against property subject to the effective control of the defendant if the third party is a bare nominee titleholder who is acting in bad faith.

14 United States - in criminal cases, the standard of proof is that appropriate to a sentencing hearing, namely the preponderence of the evidence.

15 United States - in civil cases, if the government shows that there is probably cause to bring the proceedings, then the burden shifts to the defendant to show that he or she did not know that the property was acquired illegally or did not consent to the use of the property in an illegal manner.

ANNEX C

EVALUATION OF MEASURES TAKEN BY FATF MEMBERS DEALING WITH CUSTOMER IDENTIFICATION[1]

Introduction

1. This paper presents a synthesis of measures taken by FATF members in relation to customer identification requirements and record-keeping rules. It deals with both the identification regime set up by members and the practical problems which may have arisen.

2. The "know your customer" policy is probably the cornerstone of the forty FATF Recommendations. While all members have generally implemented the Recommendations dealing with customer identification and record-keeping, there is a need to examine the effectiveness of the identification regimes in place and to see whether some refinements are necessary in order to solve the problems encountered in the most difficult situations by financial institutions.

3. The paper first describes the customer identification and record-keeping systems in FATF members. It then addresses specific issues such as anonymous accounts, identification of the beneficial owner, identification in cases where there is no face-to-face contact between the customer and the financial institution, and future challenges linked to the development of new technologies in electronic payments such as stored value cards. Finally, the conclusion will endeavour to provide an overall assessment of the effectiveness of identification regimes and their impact on money laundering activities.

I. DESCRIPTION OF CUSTOMER IDENTIFICATION AND RECORD-KEEPING REQUIREMENTS IN FATF MEMBERS

A. IDENTIFICATION REQUIREMENTS

(i) Legal framework and guidance provided to institutions

4. In a vast majority of members, customer identification has been introduced by legislative provisions. However, two members have implemented identification requirements by decree (Turkey) or regulations (Japan). Two other members (Hong Kong, Singapore) have covered the matter with guidelines which have the force of law. In other members, the requirements for customer identification for the bulk of the institutions are provided in the law while some sectors are covered by regulations. The Netherlands is equipped with a law — the Identification (Financial Services) Act — which deals only with identification matters. Finally, in Switzerland, customer identification is dealt with both by law (the penal code punishes a lack of vigilance by financial institutions when they identify the beneficial owner) and by other norms (Due Diligence Convention of the banks, Directives of the Federal Banking Commission).

5. While most of the regimes in place were brought into effect recently (between 1990 and 1996), following the adoption of the forty FATF Recommendations, provisions in several previous laws already

[1] This document reflects information provided to the FATF Secretariat prior to 28 February 1997. Changes are continually occurring in national legislations and practices and therefore specific questions on current law and practice should be put to the relevant national authorities.

contained identification requirements. It is also interesting to note that, prior to the passage of legislation, self-regulatory guidelines were issued by the industry to provide standards for customer identification in the absence of legal requirements (e.g. Italy, Luxembourg, New Zealand, United Kingdom). In addition to the enactment of laws and regulations and the adoption of guidelines, further guidance has been provided either by the supervisory bodies or the trade associations, in all members except two for non-bank financial institutions. The nature of these further guidelines varies considerably and they do not all constitute a legal interpretation of the law.

6. All the identification regimes apply to both banks and non-bank financial institutions. However, in one member identification requirements only apply to banks. In a limited number of countries, identification requirements also apply to all or part of non-financial businesses, when they undertake financial activities (Australia, Belgium, Denmark, France, Germany, Netherlands, United Kingdom) or even when this is not the case (Portugal). In the very near future, two members (Belgium, Italy) will extend identification requirements to apply to non financial businesses.

(ii) Contents of the legal frameworks and guidance[2]

(a) Opening of accounts and passbooks

7. The types of documents which are necessary for identifying natural persons opening an account are generally, but not always, set out in circulars or guidelines (e.g. Germany or Portugal). In France, the documents necessary for identifying persons, either individuals or legal entities, are specified in statutory provisions. In Canada, the documents necessary for identifying persons are specified in the Proceeds of Crime (money laundering) Regulations. The guidelines may also contain details for establishing the identity of different types of customers.

8. The definition of the documents which should be obtained differs between countries. However, in a majority of members, it is required to present an official document or any document from a reputable source, which bears a photograph and a signature. The documents which are the most commonly acknowledged and accepted are: identity card, passport, driving licence, social security card and special card of foreigner or refugee. In some members, other documents such as a certificate of marriage, municipal identity card, military card, police card or identification card issued by banks. Moreover, the personal identification number is generally requested in Nordic countries and, for deposit accounts in the United States, a taxpayer identification or social security number must be provided.

9. It should be noted that Norway, in addition to issuing a list of documents which are deemed to have a satisfactory level of security, has issued a list of documents which are deemed not to have a satisfactory level of security. The latter list, which is not exhaustive, includes birth certificates, credit cards, travelling cards for buses and trains, membership cards of unions or school certificates. In Denmark, only documents which are difficult to falsify are accepted. In Australia, the regulations specifically provide types of documents and points to be allocated to those documents, if the "100 point" system is used. However, the decision as to whether it is necessary to undertake further verification on the authenticity of the documents is left to each "cash dealer" (financial intermediary). In fact, the system requires that at least two documents, and often three or more, are required to be sighted by the cash dealer. In almost all cases, the documents must be full and valid.

10. Even though customers should produce an original document, a number of formal checks should be conducted, e.g. verification of the signature, examination of a possible anomaly in the photograph, the

[2] Only for natural persons. The requirements for legal persons are dealt with at paragraphs 21-26.

physical appearance of the prospective customer. On the whole, financial institutions must verify that the documents presented do not show any sign of alteration. While there are various means of verifying the address, none of them are really satisfactory. Sending and receiving mail does not provide unquestionable results. Of course, further checks can be conducted on the voters roll, telephone directory or recent utility or rates bills. In Japan, the client contact officer of the financial institutions visits the clients to confirm their address. In fact, financial institutions should be vigilant when the customer is domiciled at a third party or post box.

11. Finally, further checks are also carried out in several members. In Belgium, the institutions covered by the law should obtain other information related to their customers (profession, composition of the family, research of address changes, etc.). In Singapore and the United Kingdom, whenever possible, the prospective customer should be interviewed personally. In France, a bank which opens an account to a customer who shows a suspicious haste may engage its liability. The French Banking Association recommends not to accept vague indications on professional activities. For large accounts and/or transactions to be opened and/or carried out in the United States, it is required that the customer provide identification and even prior bank references and, if appropriate, write to that bank and request a customer reference. Also it is suggested that, in this case, banks should consider obtaining a credit bureau report. In Spain, financial institutions are especially cautious in particular cases, such as the verification of an operation through an intermediary, opening of accounts to unknown or non-usual customers, accounts assigned to receive funds from abroad and to be re-transmitted to other places in relation to financial, mercantile or investment operations. In general, several members use phone calls and cross-check information which is available from other files and registers.

(b) Other operations covered by identification requirements

12. In addition to the opening of accounts and passbooks, proof of identity is generally required where a customer conducts an occasional large transaction and where a transaction is suspected of being connected to money laundering. Furthermore, identification of the customer is required in any cases of starting a permanent business relationship and for a number of operations/transactions which include: renting of safe deposit boxes; taking custody of securities, precious metals and other assets; cashing share coupons, bank certificates and similar negotiable instruments; issuing credit cards; and carrying out large currency transactions and wire transfers.

13. In universal banking systems, most financial transactions are considered as banking business and are therefore covered by identification requirements. While some members (e.g. Germany, Greece, Singapore, Sweden) have provided a list of financial transactions for which proof of identity is obligatory, others (e.g. Norway, Spain, United Kingdom) have a general requirement for all financial activities. In France, customer identification is required for the opening of any type of account (notion of usual customers) for all operations with unusual customers above a certain threshold and the renting of safes. Also, as securities are dematerialised, they are kept on accounts. In Italy, proof of identity is required for persons who undertake operations involving means of payment or transfers of bearer securities for amounts exceeding 20 million lira. It is interesting to note that in Luxembourg, the word “account” should be interpreted as broadly as possible to include all financial operations. In New Zealand, the concept of “financial facility” which is broadly defined to include any account or arrangement provided by a financial institution through which two or more financial transactions can be conducted, and the broad definition of a “transaction”, which refers to any deposit, withdrawal, exchange or transfer of funds, have effected a very wide range of financial operations. Finally, it should be noted that under Australian legislation, all international funds transfers instructions over $10 000 are covered by identification requirements. In addition, in the United States, a new regulation requires all financial institutions transmitting or receiving

domestic or international funds over a fixed threshold, to identify the originator or the beneficiary of the transfer.

(c) Particular cases

14. In almost all members, only official names are accepted but assumed names can be tolerated in a few countries. However, it is important to distinguish between the name used for the opening of the account and the name which will be used for the reference of the account.

15. Non-resident natural persons are identified on the same basis as resident customers. In addition, the verification of the identity of the customer can be obtained from a resident overseas who is the foreign verifying officer of the financial institution, a corresponding financial institution,[3] a consulate or an Embassy.

16. Children[4] are usually expected to be introduced by a relative known to the bank. Documentary evidence of the identity of the child and/or his legal representative (birth certificate, passport of one of the parents or other travel document or statements from an educational institutions) is otherwise required. In many countries, accounts opened in the names of children may only be credited or debited by their legal representatives.

17. In almost all members, the establishment of identity is normally needed in the case of occasional transactions when the amount involved is above a fixed threshold. This applies whether the transaction is carried out in one or several operations which appear to have been linked. When the total amount is not known initially, the financial institution should proceed with identification as soon as it is clear that the threshold has been reached. All FATF members but two have a threshold in place. In addition, irrespective of the sums involved, identification is carried out if the transaction is suspicious. However, identification of occasional customers may also be required in the case of dealings in gold and precious metals (Luxembourg). It is also true that some financial institutions do not even entertain occasional customers. In Spain, the law does not make any distinction between the usual and the occasional customer and therefore the same rules apply to both. In the United States, all banks can refuse to conduct a transaction if warranted.

18. The efficacy of the controls aimed at detecting smurfing practices is largely dependent on the structure and size of financial institutions, as well as on information technology and the information management methods put in place. Smurfing transactions are, of course, difficult to detect if they are carried out in several financial institutions. Some members (e.g. Sweden, United Kingdom) have included an interval of time (e.g. within three months) between transactions for smurfing control. In Germany, the Federal Banking Supervisory Office has introduced regulations on the use of automatic cash in-payment machines to combat smurfing. In the case of cash reporting systems, specific penalties can apply for structuring transactions (Australia). Finally, in the United States automated curency retrieval systems are available to detect structuring.

[3] The corresponding financial institution must, in general, be located in a FATF member or have an internationally recognised good reputation.

[4] This paragraph deals with children below the legal age.

(d) Exceptions

19. All members but five (Finland, Japan, New Zealand, Singapore) have various provisions in the relevant laws, regulations or guidance notes which exempt from the requirement to verify identity. Some of these provisions may specify categories of people who, in specific circumstances, may become signatories of accounts where they would not otherwise have adequate identifying documentation. For instance, in one member, these categories include recent arrivals in the country, certain recipients of social welfare benefits and some signatories to accounts with public companies and public authorities. Some members have no obligation to identify State organisations, State owned or public companies. Other categories of exemptions may include persons who are known to the financial institution or were already customers at the time identification requirements came into force. While there are no special exemptions provided by regulators, it is recognised that banks have sufficient discretion to make adjustments in their policies based upon their particular knowledge of certain customers. However, non bank financial institutions are not authorised to exempt certain customer transactions from identification requirements. Finally, it should also be noted that in several members (e.g. Denmark, Spain, United Kingdom) the exemptions do not apply where there is any knowledge or suspicion of money laundering.

20. In practice, most of the exemptions apply in the following cases:

- other financial institutions subject to the same identification requirements;
- life insurance policies where the annual premium, or the single premium, is the equivalent or less than specified thresholds;
- pension insurance schemes where the policy is taken out by virtue of contract of employment or the insured person's occupation and provided that the policies do not contain a surrender clause and may not be used as a collateral for a loan;
- insurance policies, and other operations pertaining to life insurance or pension schemes, provided that the payment of the premium or of the contribution is to be debited or drawn by cheque from an account opened in the customer's name, with a bank which is subject to anti-money laundering requirements.

(iii) Legal entities

(a) General rules

21. Legal entities are usually entitled to open accounts in their names. In some countries, however, this includes both companies and trusts, foundations, associations, etc. In most respects, relevant information regarding the formation of the entity is requested (certificate of incorporation or similar document, memorandum and articles of association). This information often also includes the number of registration, the name and postal address of the company, the names of the board's members as well as the management, the legal form of the entity. Most members request the production of the original document or certified excerpts from official registers.

22. For legal entities registered overseas, most members made it clear that comparable documents should be obtained as far as is practicable. However, since the standards of control vary among different countries, it is generally recognised that attention should be paid to the place of origin of the documents and the background against which they are produced. It is interesting to note that in Finland, non-resident legal persons are obliged to produce a letter of recommendation.

23. As a general principle, the identity of relevant individuals behind the entity (trustees, directors) is established in line with requirements for personal customers. For instance, in Canada, the identity of at least three persons who are authorised to give instructions with respect to the account must be verified. Furthermore, the resolution of the board of directors to open an account and to give authority to signatories on the account is generally requested.

(b) Further checks to be conducted

24. In addition to the above-mentioned requirements, several members have requested the relevant institutions to conduct further checks when identifying legal entities, since the establishment of identity of customers, who are not natural persons, gives rise to special problems. For instance, in Belgium, financial institutions are required to obtain information on the effective activity, size of the business and its financial situation. Finland, France and the United States have similar requirements. In Greece, further checks are only conducted for accounts which provide overdraft facilities. In the same way, if a legal entity requests a loan from a domestic institution in Iceland, further checks are only made with respect to the company and its legal registration in its home country. In Hong Kong and Singapore, there is an obligation to cross-check the information on legal entities with the company registry or the registry of companies and businesses. Financial institutions in the United Kingdom are encouraged to enquire at the start of the relationship about the size and nature of expected activities to be conducted through the account.

25. However, in several members the opportunity of conducting further checks is left to each relevant institution. In almost all members, there are no specific measures to be taken when accounts are opened in branches in the district of which the legal entity has neither its registered office nor significant business activity. In fact, this situation would often prompt a report of suspicious transaction (e.g. Australia, Belgium, Denmark, Germany, Italy, United States) or would provoke a thorough review (United States).

26. With regard to particular measures to be taken when the legal entity uses the services of a letter-box company, again, this situation could prompt special attention to the transaction or a disclosure of suspicions. Moreover, several members have required the identification of the legal entity itself (Belgium, Luxembourg). In Canada, all corporate accounts must be opened on a face-to-face basis. Some members have prohibited letter-box companies (France, Greece) and others (Singapore) have discouraged their use. However, there is no formal requirement in this respect in two members.

(iv) Compliance

(a) Measures in case of failure of identification

27. When the customer has not been adequately identified, various measures can be taken by the relevant institutions:

- sever the relationship with the customer (including refusal to open the account or refuse the transaction;
- block the account from withdrawals;
- make a suspicious transaction report;
- possible forfeiture of the account after a certain period of time;
- keep the record of the data concerning the identification.

28. The above-mentioned measures can apply either separately or together. For instance, after an account has been opened, a financial institution may block the funds and simultaneously make a suspicious transaction report. However, this position has been subject to criticism as incompatible with the principle of good faith in business relations.

29. For most members, in no circumstances should transactions be permitted on a account before the customer's identity has been established. However, financial institutions may discover later that the identification checks were not satisfactorily completed. In this case, the institutions should, as a minimum, be required to disclose information to the relevant authorities. This issue of severing business relations at this stage is nevertheless questionable. In fact, it is important to keep an audit trail in all cases and not to authorise withdrawals in cash.

(b) Sanctions for non compliance with identification requirements

30. The sanctions applicable to the institutions in cases of non compliance with respect to customer identification are as follows:

- fines for individuals, companies and financial institutions;
- the possibility of imprisonment for individuals (members of the board, directors, managers, employees, representatives or other persons who permanently or occasionally render services to them);
- disciplinary sanctions (warning, suspension of activity, or withdrawal of agreement in most serious cases);
- rectification of any weaknesses in customer identification as identified in the banking supervisory process;
- cease and desist, removal and prohibition and other such actions.

31. Again, the above-mentioned sanctions can be applied either in conjunction or separately. In many members, it is a criminal offence for an institution to fail to take reasonable measures to establish the identity of a prospective customer. Sometimes, not only the institutions but also their employees can be punished by fines and imprisonment according to their involvement in the offence and their position in the bank.

32. On the whole, there has been no evidence of any major deficiencies in complying with the general customer identification requirements. FATF members are satisfied with the way identification checks are applied. No prosecutions, or very few, have been brought against any financial institutions in this respect. In the few cases of inadequacy, action has been agreed with the institution concerned.

B. RECORD-KEEPING RULES

(i) Nature and contents

33. The banking sectors of all members[5] have implemented the following requirements:

- transaction records should be maintained for at least five years; and
- records on customer identification must be kept for at least five years after the account is closed.

34. In fact, for many members, the documents must be kept for a period of time of more than five years (Australia: 7 years; Germany: 6 years; Hong Kong: 6 years for banks; Italy: 10 years; Portugal: 10 years for records of transactions; Spain: 6 years). In addition, other provisions, particularly in commercial laws, may require a longer period of time for record-keeping.

35. While the application of standards record-keeping is satisfactory, the situation could still be improved in certain categories of non-bank financial institutions, such as bureaux de change, and for certain non financial businesses undertaking financial activities. In one member, record-keeping requirements only apply to banks. However, some members have implemented record-keeping rules for their casinos (e.g. Denmark, Spain, the United States).

36. In addition, the legislation on the coverage of documents related to the identification of the beneficial owners could be clarified. Finally, some members specified that failure to maintain adequate record-keeping systems is an offence (Ireland, Singapore)

(ii) Storage of documents

37. The way the documents used in the process of identification and the records of transactions are retained and stored is essential for a reasonably speedy and practical retrieval. Very often the laws and regulations do not contain any provisions concerning the way the documents should be stored. However, in some members (e.g. Finland), financial institutions are required to organise their record-keeping in a centralised manner so that the information may be examined later without unreasonable delay, for example, by using a register or reference number. With regard to the contents of the information, it is interesting to note that in Norway the name of the officer within the financial institution who receives the information, must be furnished along with the identification information.

38. The storage of documents in a “paper format”, sometimes in various locations, makes ready access very difficult, especially after the termination of business relations (documents stored in central warehouses of the financial institution and not at branches. The various forms of electronic storage (microfilm, optic disks, computerised forms, etc.) can ease this situation. However, for legal reasons and evidentiary purposes, it seems that usually the originals of certain documents (certified copies of the originals) are still required, and therefore must be retained in their original form. In this respect, it is necessary to find the right balance between the need to keep either the original document or copies admissible in court proceedings, and the standard procedures of financial institutions which seek to reduce the volume of records which need to be stored.

[5] However, one member does not have specific requirements regarding the retention of records on customer identification. While financial institutions maintain such records, in practice, consideration is being given to amending the regulations to require the recording of information on customer identification.

39. The retrieval of documents pertaining to occasional customers may be more problematic. In order to solve this difficulty, one member (Belgium) has established a "modus vivendi" to specify the requests for documents (identity, region and time of the transaction, etc.). In most members the documents are accessible within a reasonable time, in particular if the handling branch and the account number are known.

(iii) Access to stored data

40. In general, documents relating to transactions and the account identification process are accessible by all law enforcement agencies, financial regulators and judicial authorities. The means by which they can be accessed varies with the type of powers available to the afore-mentioned authorities and the context of the investigations. In general, the police need a search warrant or a subpoena to access customer identification data.

41. The financial regulatory authorities have access to the identification documents of the financial institutions without limitations although in some cases only for supervisory purposes. In some members, the disclosure receiving agencies have also unlimited access provided that a suspicious transaction report has been made. Sometimes, all the above authorities, including the police, have access to customer identification records without a search warrant (Iceland). In another extreme situation, the supervisory bodies, law enforcement and judicial authorities, may be required to justify access to the archives by means of a formal request.

II. SPECIFIC ISSUES

A. ANONYMOUS ACCOUNTS

(i) Description of the requirements

42. Financial institutions in FATF members are not permitted to open anonymous accounts or accounts in fictitious names. This requirement can be based on either specific legislative or regulatory provisions (Australia, Germany, Greece, Japan, Luxembourg, Singapore). However, in most cases, the objective of the FATF Recommendation to prevent anonymous accounts and accounts in fictitious names is a direct consequence of the general customer identification requirements. In other words, the prohibition applies to all types of accounts, safe deposit boxes and passbooks, with the exception of one member for the latter. There are various administrative, civil and penal sanctions in cases of non compliance.

43. In almost all members, the scope of the prohibition includes anonymous accounts which may be offered via new electronic systems such as Internet. However, the requirement does not apply to service providers established overseas. This situation gives rise to problems when a foreign country does not apply the FATF Recommendations, and in particular those relating to customer identification. In one actual case, an offshore bank based in the Caribbean proposes the opening of anonymous, coded and numbered accounts through Internet.

44. Due to the potential risks involved in technological innovations such as Internet banking, several members have indicated that they are considering an appropriate policy response (Australia, Hong Kong, Portugal). The latter considers that if its home country regulations prove ineffective, and if the number or size of the balance of those accounts so justifies, it will consider enacting legislation to prevent residents in Portugal (natural or legal persons) from opening anonymous accounts offered by foreign institutions via Internet.

(ii) Exceptions

45. The most important and serious exception to identification requirements relates to the passbooks which can be opened anonymously by Austrian residents. It should be noted that Austria recently decided that no new anonymous securities accounts could be opened after 1 August 1996.[6] However, the possibility of opening anonymous passbooks still exists and continues to be a matter of serious concern. Seven years after joining the FATF, Austria is still not in full compliance with Recommendation 10. Failure to take action in this area could undermine the Austrian system for fighting money laundering.

46. There are also several other specific situations which, nevertheless, do not affect the implementation of "know your customer" principles. In Italy, although only bearer securities deposits can be attributed to fictitious names, the financial institutions are, in any case, required to ascertain the identity of the persons opening, closing or conducting transactions on these accounts. In France, cash purchases of capitalisation bonds from insurance companies or (bank-issued) short-term notes are unrestricted and anonymous for tax purposes. However, financial institutions are required to identify clients who purchase or redeem such bonds or notes and the preservation of client anonymity cannot be evoked as grounds for non disclosure to TRACFIN (Traitement du renseignement et action contre les circuits financiers clandestins).

47. In Belgium, in exceptional and specific cases which require discretion (key public figures, managers of the bank, etc.), the bank employees do not know the identity of the customer. It is therefore permitted to open numbered accounts or accounts in assumed names but only for these categories of clients. However, the identification of the customer is always verified at the management level of the bank and the latter is, of course, obliged to communicate the true identity of these account holders in cases of investigation or suspicious transactions reporting.

48. No anonymous accounts or safe deposits are permitted in Switzerland. However, as a further internal security measure, banks can open accounts or safe deposit boxes under a number or a pseudonym. This allows a limited number of bank staff to have access to the true identity of the holders of numbered or coded accounts. In any case, the banks are required to identify the actual account holder and the beneficial owner, if any.

B. IDENTIFICATION OF BENEFICIAL CUSTOMERS

(i) General requirements and cases where customers are represented by non-financial businesses, particularly lawyers

(a) General

49. In almost all members, financial institutions are required to take reasonable measures to obtain information about the true identity of the person on whose behalf an account is opened or a transaction is conducted (beneficial owner), if there are any doubts as to whether the client or customer is acting on his own behalf. However, there is one exception for non-bank financial institutions in one member.

50. In general, with regard to life insurance products, several members (e.g. Finland, France, Italy, Netherlands) have implemented various measures to identify, not only the policy holder but also the beneficiary of the contract. Due to the nature of life insurance contracts, the beneficiary may not be

[6] For existing securities accounts, securities are only permitted to be sold anonymously from 1 August 1996 onwards.

known at the time the policy is taken out and the identity of the beneficiary may therefore only be verified at the time payment is made.

51. Non-financial businesses are not always required to identify beneficial customers, especially when financial business is not their main activity. In most cases, there are no specific identification rules when customers are represented by non-financial professions. Some members have included certain categories of non-financial professions in the scope of the measures concerning customer identification (e.g. lawyers in Denmark; casinos, businessmen when carrying on their trade or business, and persons who administer another person's assets against payment in Germany; lawyers in New Zealand). In Norway, in cases where a customer is represented by a lawyer or other non-financial profession, the institution shall seek to obtain complete identity information about the person on whose behalf action is being taken.

(b) Non-financial businesses and lawyers

52. The general obligation to identify both the customer and his representatives (FATF Recommendation 11), irrespective of their professional capacity could probably address these specific cases. However, several non-financial businesses are characterised by a duty of professional secrecy (lawyers, accountants, bailiffs) which may prevent them from revealing the identity of their clients.

53. To solve this difficulty, various measures have been implemented. In Belgium, the non-financial intermediaries acting on behalf of their clients, should sign an attestation stating that no money laundering is involved. In the case of refusal, financial institutions should not execute the operation and should report the case to the CTIF (Cellule de traitement des informations financières), if the circumstances of this refusal show any indication of an attempt to launder. Conversely, should an intermediary sign such an attestation knowing that the funds are derived from one of the money laundering underlying offences, its penal and disciplinary liability would be engaged.

54. A section in the Irish guidance notes deals specifically with non-financial intermediaries (e.g. solicitors, accountants, etc.). If the financial institution is satisfied with the bona fide of the intermediary, the identity of the third party can be established by receiving a name from the intermediary. This can only be relied upon where the intermediary has given a written undertaking that it will take reasonable measures to establish identity, will retain documentary evidence and will, upon request, furnish a copy of the information to the financial institution. In any case, where it appears that the intermediary is merely providing a "front", such an undertaking will be inadequate and identification of the third party must be established by the financial institution.

55. When customers are represented by lawyers or any other non-financial profession, the financial institutions in Singapore require the production of the identity card or passport of the beneficial owner and they also check that the lawyer or professional concerned is duly registered locally. In Spain, if the client acts through a lawyer or another person, the latter must be identified by proving the power of attorney which enables him to act on the client's behalf. In Turkey, when a natural or legal person conducts a transaction with a bank on behalf of another person, he/she is required to submit a proxy statement arranged by a public notary for that specific transaction, certifying the identification of the beneficial owner. This rule applies whoever the representative is (trust, lawyer or other non-financial profession).

56. In Switzerland, while the banks which are subject to the Convention of Due Diligence are required to identify the beneficial owners (obligation to fill in "form A"), there are some exceptions for accounts or deposits established in the names of lawyers or notaries. These exceptions only apply in cases of payment of professional or judicial fees or deposits of patrimonial values and their related investments regarding inheritance, divorce or in trial cases. These situations are certified by written statements by lawyers and notaries.

57. Several members have also adopted measures to deal with situations where there are doubts as to the accuracy of the information pertaining to identification provided by non-financial businesses. In the case of serious doubts or when identification cannot be established, financial institutions can always refuse to open the account or execute the transaction (e.g. Germany, Switzerland). In Luxembourg, in a case where there is doubt that a customer is acting on his own behalf (because the customer is a legal entity which can form a "front": holding, Anstalt, trust, etc.), the latter is asked to provide a written declaration stating that he/she is acting for himself or establish the identity of the beneficial owner.

58. While banks cannot always establish the identity of the person(s) for whom a solicitor or accountant is acting, two members have indicated that this does not preclude banks from making reasonable enquiries about transactions passing through clients or beneficial accounts which give cause for concern, or from reporting those transactions if any suspicions cannot be satisfied. In the United Kingdom, where a money laundering enquiry arises in respect of such a client account, the law enforcement agencies will seek information directly from the intermediary as to the identity of the underlying client and the nature of the relevant transaction. The United Kingdom Money Laundering Guidance Notes recognise that there can be even more complex money laundering situations where the intermediary is from a country without equivalent anti-money laundering legislation. Of course, reasonable measures should again be taken to verify the identity of the underlying client. However, if it becomes apparent that the intermediary is playing little or no role beyond providing a "front", full verification procedures become necessary if the account opening is to proceed.

59. Finally, and this is certainly the best way to deal with this problem, several member governments have proposed to include categories of non-financial businesses in the scope of their anti-money laundering legislation (Australia: lawyers; Belgium: notaries and bailiffs). The Italian government intends to extend identification requirements to parties undertaking activities "particularly susceptible to be used for money laundering purposes due to the fact that there is an accumulation or transfer of major economic or financial resources, or that there is a risk of infiltration by organised crime."

(ii) Beneficial customer of trusts or nominee account holders

60. The most complex situations are found when customers are represented by trusts or nominees, especially when the latter are domiciled overseas in poorly regulated countries. The responses to these situations vary among the membership. Firstly, in some members (France, Spain, Portugal) trusts do not legally exist. Several members have specifically included trusts or nominee account holders in the scope of their laws, regulations or guidance notes dealing with customer identification (Australia, Denmark, Ireland, Italy, Japan, Luxembourg, New Zealand, Norway, Sweden, Switzerland, United Kingdom, United States). This inclusion can be either direct, with the trust or nominee account holders being treated as a financial institution or business, or indirect with a specific requirement for financial institutions to identify the beneficial owners.

61. However, it seems that the nature of such requirements differs from the general customer identification regime. In almost all members, where applicable, it is not mandatory to identify the name of each beneficiary of a trust. In fact, verification by a financial institution of the identity of the person acting as trustee, nominee or fiduciary does not raise specific problems. However, it is of course more difficult to identify the parties for whom the trustee or nominee is acting and to seek confirmation that the source of funds or assets under the trustee's control can be vouched for. According to the United Kingdom Guidance Notes, if the applicant is unable to supply the information requested, enquiries should be made as to the identity of the person who has actual control and the results should be recorded in the account opening file.

62. It is generally recognised that the reasonable measures undertaken to obtain information concerning the underlying beneficiary need to take into account legal constraints and/or good market practices in the respective area of activity, the geographical location of the trustee and beneficiaries to which the trust account relates and, in particular, whether it is normal practice in those areas or markets, to operate on behalf of undisclosed principals. In New Zealand, in order to take into account the practical difficulties associated with the identification by financial institutions of the beneficial customers of domestic trusts or nominee shareholders, this requirement has been limited to cash transactions involving NZ $ 10 000 (approximately US$ 7 000) or over. In Hong Kong, it is proposed to strengthen the guideline of the Monetary Authority by including the requirement that banks should verify the identity of trustees, nominees or account signatories as well as the nature of their trustee or nominee capacity and duties, for example, by obtaining a copy of the trust deed. In a case where the beneficiaries cannot be identified, the proposed revised guideline would require banks to pay special attention to business relations and transactions with the customer, including monitoring activity of the account in question.

63. It is generally admitted that trusts created in poorly regulated countries or jurisdictions, or the use of offshore investment companies, deserve special attention. However, while several members recommend that financial institutions undertake additional enquiries as to the true identity of the beneficiaries and sometimes also on the source of the funds, there is probably no fully satisfactory solution in this respect.

C. IDENTIFICATION IN CASES OF NO FACE-TO-FACE CONTACT

(i) Requirements in place and identification methods

64. In most members' legislation or regulations, there are no provisions which deal specifically with cases where there is no face-to-face contact between the financial institution and the customer. Therefore, in many members, financial institutions are required to obtain copies of identification documents, irrespective of the way the financial products are distributed. However, recognising the difficulties posed for customer identification in cases of mechanisms which avoid face-to-face contact between financial institutions and their clients, several members have addressed this issue in their guidance notes, circulars or instructions.

65. In general, face-to-face contact would normally be required. In Canada, it is even required that there must be face-to-face contact (verification in person) in the case of direct banking and direct insurance writing. However, the following paragraphs describe measures which have been implemented in member countries and practical solutions in cases where business is conducted by post, telephone or electronically.

(a) Direct banking

66. Firstly, where the transactions[7] are carried out by a distance selling institution, payments should be made via or to the customer's bank account opened in another institution. It is expected that identity checks have already been carried out by the latter. However, there is still no proof that the customer has been correctly identified. Moreover, it seems difficult to transfer the liability for identification from the distance selling institution to the institution which holds an existing account.

[7] Payment made for a financial service or benefit (interest, insurance premium, etc.) provided by a financial product.

67. The Identification (Financial Services) Act in the Netherlands authorises the Minister of Finance to designate cases for which the identification requirements are fulfilled when it is established that the first payment from the client is to be debited from, or is to be credited to, an account opened in the customer's name with a bank in the Netherlands or in another country designated by the Minister of Finance. The Minister of Finance has used this authority to designate direct banking services. The financial institution is required to obtain confirmation from the customer's bank that the client has been properly identified and that the client's identity has been recorded by the said bank.

68. There are various procedures to check the personal identification and verify the address of the applicant. In many instances, the distance selling bank demands a copy of a relevant identification document. In Germany, notaries public and other banks are authorised to establish identity on behalf of the institution obliged to identify the customer. The data and the copies of identification documents must be certified as official by various authorities1 : police, consulate, notary, Embassy, etc. (Luxembourg); lawyer, auditor or public notary (Norway, Portugal). In Portugal, the information relating to a customer must also be certified, in writing, by a bank established in a European Union member State, in a FATF jurisdiction or by a bank of internationally recognised good reputation.

69. In several members, where the account is opened by post, various mechanisms for checking the address and sometimes the name of the customer, are applied: sending documents by registered mail (Norway, Portugal) with the acknowledgement signed personally by the account holder (Austria) or by simplified registered mail with the absence of return being deemed as a verification of the customer's identification (Japan), surveillance of the mail or exchange of correspondence (Belgium, France, Switzerland), applying the identification requirements for banks by counter staff at the premises of the post or in the course of mail delivery (Germany), prohibition of the use of Post Office boxes (Spain).

70. Further methods of verification include: checks on the Voters Roll or providing original gas or electricity bills (e.g. United Kingdom). In addition, it is recommended that banks cross-check the information with other available information from the national register office, the tax office and the Register of Enterprises (Norway) or any public register (Sweden). In the latter country, the prospective customer will often be requested to visit a branch office before entering into business relations with the financial institution in question. Other forms of verification can include a telephone call to the applicant (at home and at work), to establish that the details are correct (Belgium, Spain, Sweden, United Kingdom). In the United Kingdom, the applicant's employer is also contacted, for independent confirmation.

71. Other specific provisions applicable to the opening of bank accounts by correspondence which also minimise the risks which are linked to a non face-to-face identification, are as follows:

- such accounts can only be credited with cheques or transfers from another pre-existing account (Belgium, Canada,[9] France);

[8] However, this solution may be seen as too costly and burdensome.

[9] At present this applies only in the case of securities dealers. The regulations allow identity to be verified by confirming that a cheque drawn by the client has been cleared or by confirming that the client holds an account at a Canadian deposit-taking institution. Consideration is being given to modifying the identification requirements along these lines.

- the prohibition of cash and cheque withdrawals from these accounts; only transfers to other accounts are permitted (Belgium);

- cross-checking information on the copies of identification documents with the sources of the information;

- paying particular attention where such accounts are opened by persons from abroad, and where the account is supplied by large wire transfers from another country (France);

- direct selling banks do not carry out one-off transactions (United Kingdom);

- in the case of the delegation of identification checks to a third party, the framework of the delegation should be precisely defined and the partners or correspondents[10] should be adequately qualified.

(b) Direct issue of credit cards

72. With regard to issuers of credit cards, the situation is a little different. In this case, the credit card issuer often requires its clients to mandate the issuer to transfer payments from a pre-specified bank account of the client to the account of the credit card company. As an additional safeguard, credit card issuers usually ask a potential client to mail to them a recent bank account statement in his name regarding the account to be debited.

73. Consequently, this situation raises less difficulty. In addition, some of the checks conducted in the case of direct banking (see above), can also apply to the direct issue of credit cards (e.g. monitoring and checking the mail). In general, for the issuance of credit cards, identification checks are naturally strict because cardholders may be subject to income qualification and credit limitations on applications for credit cards.

(c) Direct insurance writing

74. Although traditional life insurance and other related investment products may not be commonly sold at distance, the recent development of standardised life-insurance, which can more easily be sold by correspondence, has been addressed by a few members, as follows:

- the identification process is deemed to have been fulfilled when it has been established that the premiums can be settled through an existing account of the insured person at an authorised financial institution[11] provided that the third party or beneficiary has been fully identified;

[10] For instance, in Luxembourg, the partners can only be financial institutions established in that country or institutions located abroad which are subject to prudential supervision by a competent authority.

[11] However, in such cases, there should be a companion requirement to maintain the relevant records concerning details of the account number and authorised financial institution, etc. (cf. United Kingdom Guidance Notes).

- the documents related to the contract can be sent by registered mail with various additional checks on the addressee;

- in addition to traditional identification information, applicants can be asked to produce other documents such as medical certificates, etc.

(d) Nominee securities accounts

75. In general, the applicable laws and regulations require reasonable measures to be taken to ascertain the identity of the agent or the intermediary's principal. The bio-data of the applicant must be verified by a public notary and the financial institution should rely on its overseas branches or correspondents to ensure that the applicant is in fact the said person (Singapore). In the United Kingdom, if the intermediary is himself subject to either the regulations or "equivalent provisions" regulated overseas, then a written assurance may be accepted that the intermediary has obtained and recorded the principal's identity under his own procedures. Laws and regulations can also require that any agreement, involving the receipt of funds for investment in securities or other valuables for the customer's own account, will be made in the name of the client, legal or physical person (Iceland). In Switzerland, the customers of nominee securities accounts can also be registered as beneficial owners. The nominee has a complete list of customers with their names and addresses.

(ii) Alternative or complementary methods in cases of no face-to-face identification

76. In general, there are no special mechanisms which require banks to monitor accounts opened by distance selling, perhaps because distance selling or the acquisition of accounts or deposits are not so common. Apart from the general obligation for financial institutions to pay special attention to accounts opened by distance selling (e.g. Denmark, France), no specific monitoring mechanisms have been implemented in such cases except in Australia and Belgium. In the former, transnational activity is monitored for some accounts, but only with respect to significant cash transactions reports, international funds transfer instruction reports and suspicious transactions reports. Some banks in Belgium have implemented internal control measures in this respect (i.e. automatic systems for the detection of large movements and the establishment of a daily list of all withdrawals, suspicious operations may trigger a visit to the client, and non residents' accounts must be closely monitored).

77. In some member countries, banks have set up computer programs relating to "unusual" behaviour of an account (Australia, Italy, Spain, United Kingdom). However, in most respects, these have only been developed by a few banks and an even more limited number of non bank financial institutions. In the United Kingdom, a number of plastic card issuers have used or developed expert systems to prevent and detect fraud. These systems could also be used for anti-money laundering purposes but the routine profiling of customer's accounts and the monitoring of exceptions reports are seen by the United Kingdom financial institutions as more useful and cost-effective in the detection of money laundering than expert systems.

(iii) Reliance on photographic identification

78. In cases where there is no face-to-face contact, because customers can only be asked to supply copies of identification documents, the security provided by photographic identification may be questionable. In this context, several members believe that the risk of forgery is too great due to the universal availability of sophisticated copying and desk-top publishing systems, which can render the use of copied documents wholly unreliable.

79. Many other members also recognised that it is not entirely safe nor helpful to rely exclusively on photographic identification in situations where there is no face-to-face contact. Therefore it is most important to implement the measures which are set out in the paragraphs dealing with direct banking, as well as provisions which clearly state that documents which show obvious signs of alteration should not be accepted.

80. Some members are equipped with centralised data systems, or identification documents (e.g. Hong Kong, the Netherlands) or regulations requiring a national registration number (e.g. Denmark). While these measures can help financial institutions to identify national customers in a case of no face-to-face contact, they do not address the situation of overseas clients. A possible solution, which has already been mentioned in paragraph 68, are certified copies (by an attorney, consulate or embassy) of identification documents, if the bank has no branch/subsidiary in the applicant's country of residence.

(D) FUTURE CHALLENGES REGARDING SMART CARDS

(i) Identification requirements applicable

81. The use of stored value cards as a means of payment has not yet become generalised in all FATF members. These cards do not yet exist in ten member countries (Iceland, Ireland, Greece, Japan, Luxembourg, New Zealand, Norway, Singapore, Turkey) and have only recently been introduced in

others. In most of the former, relevant projects are being experimented. The regime of authorisation for the issuers of such cards is quite strict, as the latter must be issued either by banks or credit institutions which are subject to customer identification, or by credit card companies which are subject to special authorisation by financial regulators or central banks (e.g. Denmark, Portugal, Singapore). In addition, and in all instances, the amount which can be stored on the cards is limited and this may reduce their vulnerability for money laundering purposes.

82. In fact, in a majority of cases, stored value cards are, or will only be issued by banks or other institutions which are, themselves, already covered by customer identification requirements (e.g. Australia, Austria, France, Germany, Hong Kong, Italy, Portugal, Singapore, Sweden, Switzerland). In Belgium and the Netherlands, stored value cards should necessarily be linked to a bank account which would imply that identification procedures apply. Normal identification procedures would also apply to the issuance of the cards in several members (e.g. Luxembourg, Spain, United Kingdom, United States).

83. Denmark has recently introduced legislation dealing with the issuance of prepaid cash cards. The issuers of the cards are under the supervision of the Danish Financial Supervisory Authority except for cards with a value under DKK 500 (approximately US$ 80). The legislation does not prescribe any identification requirement to individuals or companies buying prepaid cards, but the issuers must keep a register of all cards in circulation. Such registers can contain useful information for security purposes (the balance outstanding on a cash card, counterfeit cards, card used for a total exceeding the value).

(ii) Record-keeping requirements

84. Some FATF members are confident that an adequate track of the transactions which are carried out by stored value cards, particularly for large transactions (Australia) or for any kind of transaction (France), would be maintained, because the general anti-money laundering requirements would apply. This is probably true where stored value cards are issued and managed by banks.

85. Although the re-loading of smart cards is ultimately made through the debit of a bank account, they can be used by anyone, anywhere, and for whatever reasons, in the same way as any other bearer means of payment, especially for the multi-purpose smart cards. There is therefore no effective means of keeping track of the relation between the bank account holder and the card holder.

86. It is in fact possible to keep track of the bank account which is debited if the card management company regularly reports to every issuing institution all the transactions which have been settled through each card. It would also be interesting if the amounts loaded in a card could be registered in a central database. Maintaining a central database of transactions, or data retrieval capacity, would allow the participating banks to monitor transactions. Furthermore, where cards are not linked to a bank account, both the loading operation and the subsequent payments are anonymous, so that no paper trail is generated. This problem could of course become more acute if purse-to-purse transactions are allowed.

(iii) Assessment

87. It is probably too soon to assess definitively the potential of money laundering vulnerabilities implied by the development of stored value cards. However, the situation should be kept under close review, especially if stored value card technology is used at some point in the future, to handle large commercial transactions.

88. The advent of stored value cards could create a convenient vehicle for money launderers to transport and transfer money without having to carry a huge bulk of cash. It is therefore important that there are regulations in place which require card issuers set up adequate anti-money laundering procedures, for example, by having an audit trail to keep track of the transactions; limiting the amount that can be transferred to and from the card, linking the card to specific bank accounts for the purpose of downloading and off-loading of value; monitoring the behaviour of card transactions; and reporting any suspicious activities related to the use of these cards.

Conclusion/Overall assessment

89. On the whole, identification regimes in FATF members are deemed satisfactory. There is no doubt that customer identification requirements have a substantial deterrent effect. In this respect, the strict application of identification checks by the banking sector has caused a shift in money laundering activities to other sectors such as bureaux de change. However, since identification regimes are only one aspect of anti-money laundering programmes, it is difficult to quantify the impact which they have on global money laundering activity. Beyond preventing money laundering, identification regimes also combat other types of crime as well as preventing the institutions from fraudulent transactions. Much has been done in the area of customer identification over the last six years, but the measures in place need to be kept under review and improved.

90. In addition to technical problems linked to the structuring of large cash transactions and the reliability and security of identification documents, the difficulty for financial institutions to verify the identification of certain types of customers or transactions is recognised in cases such as:

- legal entities, especially overseas private companies;
- shell companies, trusts and nominee accounts;
- the structuring of large cash transactions;
- customers represented by intermediaries which are non-financial businesses subject to professional secrecy; and
- situations where there is no face-to-face contact between the customer and the financial institution.

91. Although there have been some complaints about the costs of identification and record-keeping requirements, the latter definitely contribute to the prevention and detection of money laundering. However, many of the identification procedures are merely extensions of procedures which had already been established by the financial institutions for their own purposes. In a majority of cases, there are no cost estimates on how customer identification requirements are being fulfilled. However, one may consider that the costs are reasonable taking into account the FATF's objectives and the necessity of customer identification to accomplish these objectives. On the whole, it is recognised that the costs should not be overestimated. However, the duplication of identity verification across the financial sector and the costs involved by record-keeping measures could be reviewed.

92. In fact, the issue of costs should be dealt with in the generalisation of identification regimes world-wide. FATF Recommendations dealing with customer identification and record-keeping should become global standards. Another issue for future consideration is the application of identification measures in the context of the rapid development of electronic transactions and financial services through new technologies. It is also obvious that this challenge should be addressed at the international level and could be subject to further in-depth review by FATF.