FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING
GROUPE D'ACTION FINANCIÈRE SUR LE BLANCHIMENT DE CAPITAUX

1996-1997 REPORT ON MONEY LAUNDERING TYPOLOGIES

February 1997

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 A$ 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. The Principle Sources of Illegal Proceeds

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.

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 microchip, as the chip provides greater security and is portable. Microchips are much more difficult to

---

[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.

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?

---

[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.

(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.

(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.

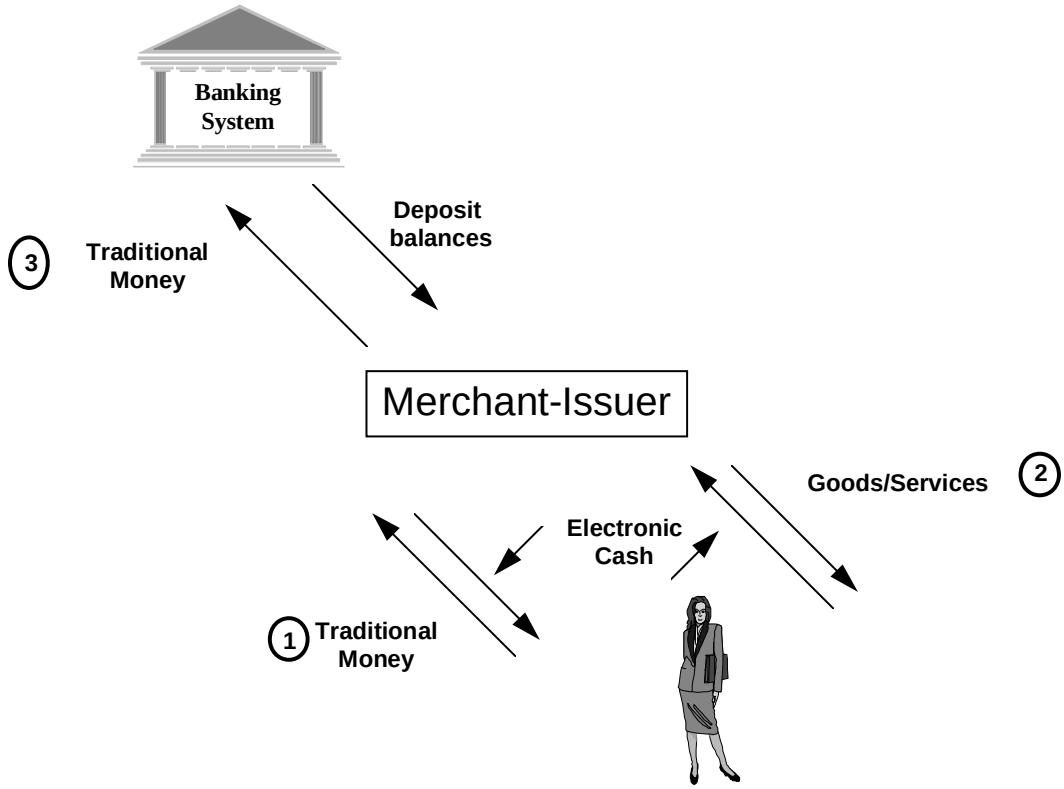
E-MONEY SYSTEMS ATTRIBUTES
SOME SIMPLIFIED GENERALIZATIONS FOR DISCUSSION*

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:

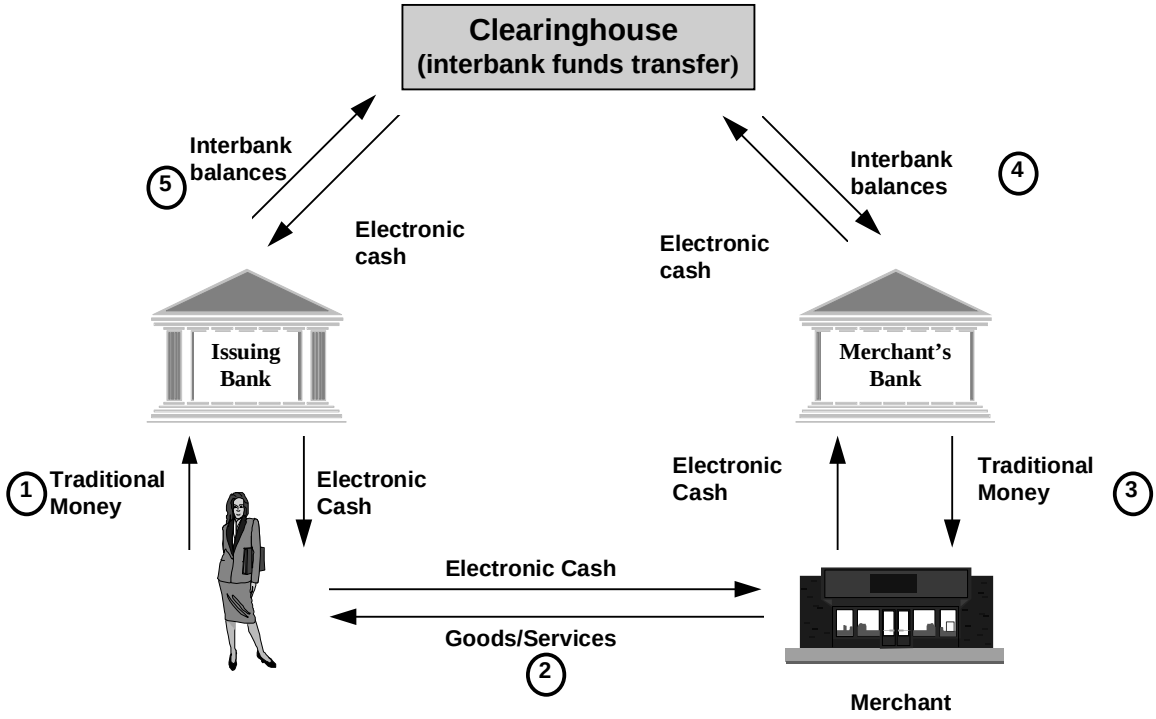
Source: Cyberpayments: An Introductory Survey, FinCEN, September 27, 1995

E-Money System:
Merchant-Issuer Model*
(Diagram 1)



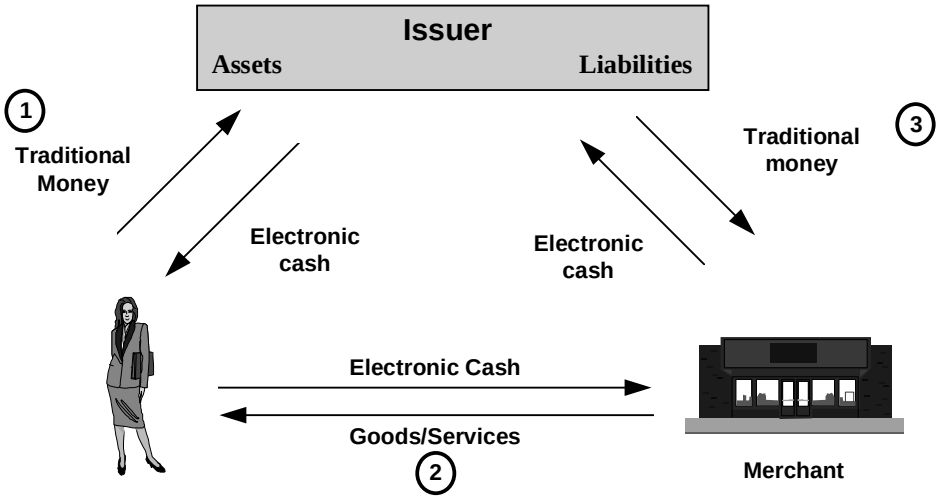
*This example refers to the United States and is included for illustrative purposes only.

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



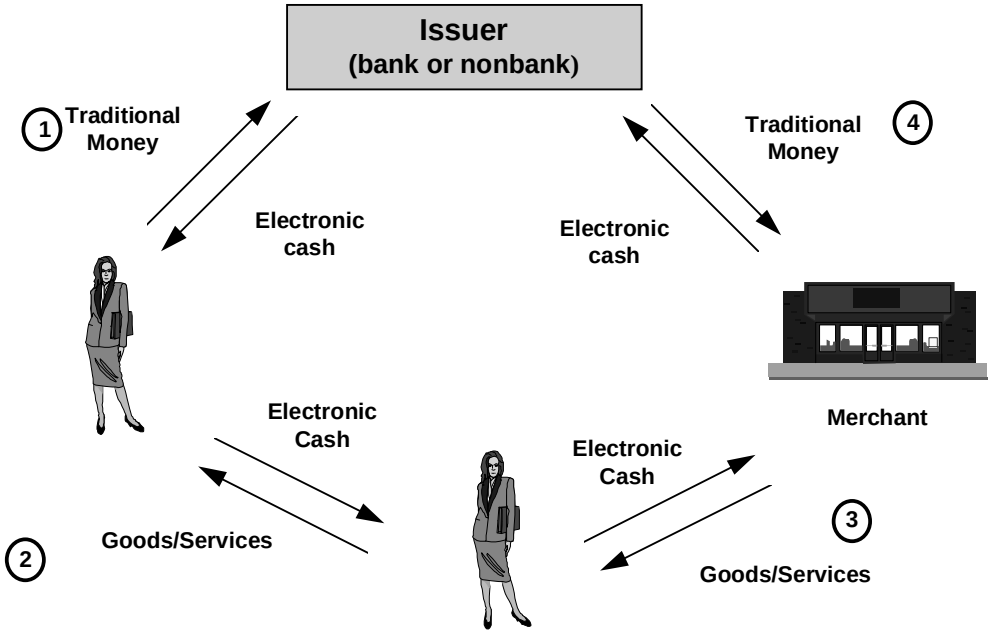
*This example refers to the United States and is included for illustrative purposes only.

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.